A Privacy-Preserving, Context-Aware, Insider Threat Prevention and Prediction Model (PPCAITPP)

By

Solomon Mekonnen Tekle

Submitted in accordance with the requirements for the degree of

DOCTOR OF PHILOSOPHY

In the subject

Information Systems

At the

University of South Africa

Supervisor: **Professor Keshnee Padayachee**

Co-Supervisor: **Dr. Million Meshesha Beyene**

July 2018

ACKNOWLEDGMENTS

I would like to express my warm and sincere gratitude to my supervisor, Prof Keshnee Padayachee, for both her guidance and support in this research and her patience in helping me complete this thesis.

I am also grateful to my co-supervisor, Dr. Million Meshesha, for his ideas and guidance.

My thanks also goes to my friends and colleagues who supported and encouraged me in my study, including Daniel Yilma, Melkamu Beyene, Fasika Tesfaye, Mesfin Gezehagn, Girma Aweqe, Dawit Mulugeta, Fresenbet Adela, Asefa Motle, Getnet Motle, Endegena Gedlu, Jacob Alemu, Dawit Demisse, Nebyou Azanaw, Melkamu Beyene and Derib Erget.

Especially, I would also like to thank my mother, Kulle Wordofa. She has been extremely supportive and encouraging.

Last but not least, I would like to thank my employer, Addis Ababa University and Ministry of Education of Ethiopia, for sponsoring my study.

DECLARATION

I declare that *A Privacy-Preserving, Context-Aware, Insider Threat Prevention and Prediction Model* is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

_____ 21, September 2017

Solomon Mekonnen Tekle Date

ABSTRACT

The insider threat problem is extremely challenging to address, as it is committed by insiders who are trusted and authorized to access the information resources of the organization. The problem is further complicated by the multifaceted nature of insiders, as human beings have various motivations and fluctuating behaviours. Additionally, typical monitoring systems may violate the privacy of insiders. Consequently, there is a need to consider a comprehensive approach to mitigate insider threats. This research presents a novel insider threat prevention and prediction model, combining several approaches, techniques and tools from the fields of computer science and criminology. The model is a **P**rivacy-**P**reserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction model (PPCAITPP). The model is predicated on the Fraud Diamond (a theory from Criminology) which assumes there must be four elements present in order for a criminal to commit maleficence. The basic elements are pressure (i.e. motive), opportunity, ability (i.e. capability) and rationalization. According to the Fraud Diamond, malicious employees need to have a motive, opportunity and the capability to commit fraud. Additionally, criminals tend to rationalize their malicious actions in order for them to ease their cognitive dissonance towards maleficence. In order to mitigate the insider threat comprehensively, there is a need to consider all the elements of the Fraud Diamond because insider threat crime is also related to elements of the Fraud Diamond similar to crimes committed within the physical landscape.

The model intends to act within context, which implies that when the model offers predictions about threats, it also reacts to prevent the threat from becoming a future threat instantaneously. To collect information about insiders for the purposes of prediction, there is a need to collect current information, as the motives and behaviours of humans are transient. Context-aware systems are used in the model to collect current information about insiders related to motive and ability as well as to determine whether insiders exploit any opportunity to commit a crime (i.e. entrapment). Furthermore, they are used to neutralize any rationalizations the insider may have via neutralization mitigation, thus preventing the insider from committing a future crime. However, the model collects private information and involves entrapment that will be deemed unethical. A model that does not preserve the privacy of insiders may cause them to feel they are not trusted, which in turn may affect their productivity in the workplace negatively. Hence, this thesis argues that an insider prediction model must be privacy-preserving in order to prevent further cybercrime. The model is not intended to be punitive but rather a strategy to prevent current insiders from being tempted to commit a crime in future.

The model involves four major components: context awareness, opportunity facilitation, neutralization mitigation and privacy preservation. The model implements a context analyser to collect information related to an insider who may be motivated to commit a crime and his or her ability to implement an attack plan. The context analyser only collects meta-data such as search behaviour, file access, logins, use of keystrokes and linguistic features, excluding the content to preserve the privacy of insiders. The model also employs keystroke and linguistic features based on typing patterns to collect information about any change in an insider's emotional and stress levels. This is indirectly related to the motivation to commit a cybercrime. Research demonstrates that most of the insiders who have committed a crime have experienced a negative emotion/pressure resulting from dissatisfaction with employment measures such as terminations, transfers without their consent or denial of a wage increase. However, there may also be personal problems such as a divorce. The typing pattern analyser and other resource usage behaviours aid in identifying an insider who may be motivated to commit a cybercrime based on his or her stress levels and emotions as well as the change in resource usage behaviour. The model does not identify the motive itself, but rather identifies those individuals who may be motivated to commit a crime by reviewing their computer-based actions. The model also assesses the capability of insiders to commit a planned attack based on their usage of computer applications and measuring their sophistication in terms of the range of knowledge, depth of knowledge and skill as well as assessing the number of systems errors and warnings generated while using the applications.

The model will facilitate an opportunity to commit a crime by using honeypots to determine whether a motivated and capable insider will exploit any opportunity in the organization involving a criminal act. Based on the insider's reaction to the opportunity presented via a honeypot, the model will deploy an implementation strategy based on neutralization mitigation. Neutralization mitigation is the process of nullifying the rationalizations that the insider may have had for committing the crime. All information about insiders will be anonymized to remove any identifiers for the purpose of preserving the privacy of insiders. The model also intends to identify any new behaviour that may result during the course of implementation.

This research contributes to existing scientific knowledge in the insider threat domain and can be used as a point of departure for future researchers in the area. Organizations could use the model as a framework to design and develop a comprehensive security solution for insider threat problems. The model concept can also be integrated into existing information security systems that address the insider threat problem.

Keywords

Insider Threat, Fraud Diamond, Context-aware System, Information Security, Privacy Preservation

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Background

According to a survey conducted by the SANS Institute (2015), 74% of information security professionals (n = 770) are concerned about insider threats and a further 34% of respondents have faced insider threat attacks. In a report by International Business Machines Corporation (IBM) (2015), it was found that 55% of the threats are committed by insiders. The insider threat problem is complex and requires an integration of various approaches in order to address the problem. There are various insider threat incidences reported in the literature that include theft of intellectual property, national security information, fraud and sabotage (Moore, Cappelli, Caron, Shaw & Trzeciak, 2009).

If insider threats are not addressed effectively, it will result in negative consequences in the performance of organizations that include loss of money, damage in reputation and a poor organizational culture (Hunker & Probst, 2011). Insider threat problems are difficult to address, as the insiders have authorized credentials and knowledge about the internal workings of the organization and they are trusted by the organization. The problem is further compounded as human elements are involved which are related to their behaviour, culture (including the organization) and social factors. Privacy issues are also raised with insider threat approaches, as monitoring employees is used as one solution to mitigate insider threats, as reported in the literature (Elmrabit, Yang & Yang, 2015). However, monitoring insiders may be a threat to privacy. Therefore, the aim of this research is to propose an integrated insider threat prediction and prevention model that considers the human elements of insiders while preserving their privacy.

The most common perspective of the insider threat problem can be understood by a definition provided by Anderson and Brackney (2014). According to these authors, the insider threat can be defined as “the threat that is caused by a malicious insider who has authorized access privileges and knowledge of the computer systems of an organization

and is motivated to intentionally adversely impact an organization's mission" (Anderson & Brackney, 2014, p.63). The domain of insiders may include current employees, former employees, consultants and any other partners of the organization who have been given access to the organization's computational resources (Hunker & Probst, 2011).

According to Yayla (2011), insider threats can be classified by two aspects considering the motive of insiders being either intentional or unintentional. The former threats are committed with a plan to attack information systems of organizations for personal benefit like theft and espionage, whereas the latter refers to accidental threats without any intention to abuse the computational resource of an organization. According to Bellovin (2008), there are three categories of insider threat attacks; these are the misuse of access, bypassing defences and access control failure.

Hunker and Probst (2011) surveyed different approaches to mitigate insider threats and generally classified the approaches into three categories, namely technical approaches, socio-technical approaches and sociological, psychological and organizational approaches. Technical approaches focus on developing technical solutions ranging from policy languages to access control, monitoring, trusted systems and other means of system hardening. The socio-technical aspect endeavours to integrate the technical approaches with the sociological solutions in an attempt to direct the attention towards social issues within the insider threat problem. Examples of sociological approaches may include policies, monitoring and profiling, prediction and forensics. However, these solutions do not include psychological factors that motivate insiders to commit a crime and other organizational factors related to insider threats. Hence, there is a need to focus on the technical, social and organizational dimensions in order to propose a holistic solution to the insider threat problem.

Recently, information security (IS) researchers such as Kandias, Mylonas, Virvilis, Theoharidou and Gritzalis (2010) have attempted to map Cressey's (1953) fraud triangle to manage the insider threat problem that justifies that fraud is a subset of the insider threat problem. According to this model, there are three elements that need to be present for fraudsters to be involved in fraudulent acts, namely pressure, opportunity and

rationalization. Pressure refers to motives that motivate a person to commit a fraudulent act and opportunities are environments that are conducive to committing fraud. In addition to pressure and perceived opportunity, fraudsters need to justify the crime to avoid guilt and shame; this is known as rationalization.

Wolfe and Hermanson (2004) upgraded the fraud triangle to the Fraud Diamond by including the fourth element, 'capability' that is essential for insiders because they also need to have the skills or ability to commit a crime. In this thesis, a model based on these four components is presented in order to mitigate the insider threat which will then provide a comprehensive solution that covers the tenets of cybercrime (i.e., motive, capability, opportunity and rationalization).

Kandias et al. (2010) attempted to map the fraud triangle to address insider threat problems, considering only the three elements of the Fraud Diamond, namely capability, motivation and opportunity. They excluded the rationalization element. Their model collects information about insiders to predict at-risk insiders however there is no mechanism in the model to preserve the privacy of insiders. This may expose the personal information of insiders to intruders. This model is limited, as the rationalization component is lacking. The model also only focuses on predicting insider threats without considering the prevention techniques. The other disadvantage of the model is that it is dependent on information gathered from the insiders themselves. This information may not be accurate.

The model proposed in this research attempts to address the limitations of the model proposed by Kandias et al. (2010) by automating the collection of information about the motive of insiders using a metadata analyser while preserving privacy. The model also adds a prevention component that addresses possible insider threats.

Brown, Watkins and Greitzer (2013) attempted to predict insiders' motives to commit a crime based on the linguistic analysis of the frequency of their word usage in their electronic communication, specifically in emails. This behaviour is believed to be an indicator of the behaviour which insiders display. Such models are criticized for abusing the privacy of insiders, as email communication is used as a source of data that may

contain personal information. Their model only considers the motive component of the Fraud Diamond, excluding opportunity, rationalization and capability.

Memory, Goldberg and Senator (2013) propose a model that predicts insider threats based on their motives, determined by automatically collecting information about their computer usage like resources and devices used, as well as network and communication patterns. Their model predicts insider threats based on motive only, excluding the other elements of the Fraud Diamond, namely opportunity, capability and rationalization. This exclusion is a limitation. There is also no assurance of privacy for the collected information about insiders and their model only focuses on prediction, excluding the prevention aspect.

The rapid growth in the use of information and communication technology with challenges in information security initiated electronic monitoring in the workplace to protect business interests and avoid any legal risks with the irresponsible use of electronic resources in the workplace (Cleveland, 2008). However, electronic monitoring is problematic to employees, as their privacy may be violated because there is a risk of exposure of their personal data during monitoring.

The supporters of electronic monitoring argue that the workplace is not a private space and employees need to use the organizational resources for office purposes only (Yang, Ren, Yang & McCann, 2015) however employees expect a reasonable level of privacy. Critics of electronic monitoring argue that monitoring will harm the mutual trust between employee and employers, which, in turn, creates frustration for employees and decreases their productivity (Eivazi, 2011).

Workplace monitoring has also been used and recommended to mitigate insider threats but the approach should be implemented with due consideration of privacy issues to preserve the privacy of employees as much as possible, and also to avoid any legal implications for abusing privacy (Huth, 2013). The balance between the security of the organization and employees' privacy should be considered when developing any model to mitigate insider threat together with the organizational culture and legal environments (Kandias et al., 2010). The issue of privacy is of concern in order to prevent defamation

particularly during insider threat prediction, as insider data is limited. This may result in false positives. If the prediction is not correct, the employees' morale and trust will be affected negatively and that may, in turn, drive them to commit a malicious act because negative feelings like anger, resentment or revenge are reported in the literature as reasons to commit crime (Aquino, Tripp & Bies, 2001, 2006; Axelrad, Sticha, Brdiczka & Shen, 2013; De Cremer, 2006; Shaw & Fischer, 2005).

In this research, a privacy-preserving, context-aware, insider threat prediction and prevention model based on the Fraud Diamond is proposed. This model gathers current contexts related to employees' motives to commit a crime by gathering metadata only based on their resource usage behaviour, including their typing patterns, search behaviours, file access and logins without collecting the content, thus balancing privacy. The contextual information is gathered to study their current behaviour, as human behaviours change over time. Their resource usage is assessed to preserve their privacy, as there is no personal data or content that will be used.

The model also assesses the capability of insiders to exploit any information security loopholes by using their sophistication in terms of their range of knowledge, depth of knowledge and skill in using information resources of the organization. The capability is also assessed based on computing the number of errors and warnings generated while employees use the information system of the organization.

Thereafter based on the assessment of the component that determines whether the insiders may be motivated to commit a crime and the capabilities of insiders, the model will facilitate honeytokens to lure insiders to commit a crime. The purpose of which is to determine whether insiders will commit a crime if any real opportunity arises that may facilitate a crime. Depending on their interaction with the honeytokens, the model will implement neutralization mitigation by means of neutralization techniques (i.e. the rationalizations used by insiders to justify a malicious act) to remove any justification that employees might use to involve criminal actions. The assessment of motives and capabilities also has a learning feature regarding the new behaviour of insiders.

The model also implements situational crime prevention (SCP) techniques to remove any rationalizations for committing a crime and to design future insider threat mitigation strategies, based on the excuses that employees provide to commit maleficence. This model is not punitive in nature; rather, it intends to detect future insider threats.

1.2 Definition of key terms

This section provides scientific definitions of key terms that are used in this thesis. More detailed discussions about the terms are available in the latter chapters.

1. **Insider**: "a malicious user who has or at some time had authorization to an organization's resources and has been involved in any one of the following activities:

   • Unauthorized extraction, exfiltration of data

   • Tampering with data or resources of an organization

   • Destruction or deletion of critical data and assets

   • Eavesdropping and packet sniffing with ill intent

   • Impersonation of other users via social engineering." (Sanzgiri & Dasgupta, 2016, p.25)

2. **Insider threat**:

   "(a) Any malicious activities that cause damage to an organization's IT and network infrastructure, applications, or services;

   (b) on the part of an employee (current or former), contractor, subcontractor, supplier, or trusted business partner;

   (c) who has/had authorized access to the organization's IT assets;

   (d) and poses a significant negative impact on the information security elements (confidentiality, integrity, and availability) of the organization." (Elmrabit,Yang & Yang, 2015, p.1)

3. **Fraud Diamond:** "… is a theory which considers that although perceived pressure or incentive might exist along with an opportunity and a rationalization to commit fraud, fraud is unlikely to take place unless the fourth element is present: an individual's capability that plays a major role in whether fraud may actually occur even with the presence of the other three elements." (Wolfe & Hermanson, 2004, p.38)

4. **Privacy preservation:** "is the protection of personally identifiable information." (Ge & Zhu, 2011, p.12)

5. **Anonymization:** "is a method that addresses the risk with identity disclosure and attribute disclosure." (Saranya, Premalatha & Rajasekar, 2015, p.1741)

6. **Context:** "… is any information that can be used to characterize the situation of an entity. An entity is a person, place or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves." (Dey, 2001, p.6)

7. **Context-aware system:** "A system is context-aware if it can extract, interpret and use context information and adapt its functionality to the current context of use." (Sordo & Vaidya, 2008)

8. **Situational crime prevention (SCP):** "Situational crime prevention can be characterized as comprising measures (1) directed at highly specific forms of crime (2) that involve the management, design or manipulation of the immediate environment in a systematic and permanent a way as possible (3) so as to reduce the opportunities for crime and increase the risks as perceived by a wide range of offenders." (Clarke, 1997, p.54)

9. **Neutralization techniques:** "… refer to a prior rationalization which individuals invoke in order to convince themselves and others that their deviant behaviours are justifiable and/or excusable." (Lim, 2002, p.679).

1.3 Problem statement and purpose of this study

Insider threats have become a serious concern for organizations. This notion has been confirmed by 74% of security professionals around the world who participated in a study conducted by the SANS Institute (2015). The problem is complicated in that the same survey found that 32% of the participants responded by asserting that they do not have a security system in place to prevent the damage posed by insiders, while 66% of them stated categorically that they do not have any insider response plan in place.

A survey conducted by the IBM also reports that 55% of the threats are carried out by insiders (IBM, 2015). The insider threat problem is challenging to address, as insiders are trusted and authorized to access the information resources of the organization. The insider threat problem is complicated by sociological issues due to human nature and human behaviours that change dynamically. This makes it challenging to carry out security monitoring and auditing (Sharghi &Sartipi, 2016).

There is a need to automatically collect contextual information about insiders, as human behaviour is dynamic and unpredictable and previously collected information may no longer apply. The problem is further magnified by the issues surrounding the privacy of insiders when monitoring them as it may create stress, frustration and even lower commitment (Brown, 1996; Dhillon & Moores, 2001). This may exacerbate the insider threat problem when insiders feel violated. Current solutions to address insider threat problems are mainly dependent on monitoring employees to detect an insider threat problem. This approach is criticized for abusing the privacy of insiders by monitoring their communication in social media and emails (Brown, Watkins & Greitzer, 2013; Greitzer, Kangas, Noonan, Brown & Ferryman, 2013).

While monitoring employees could be used as one approach to mitigate insider threats, it should be used with care to ensure that insiders' data will not be exposed to unauthorized users to be used for fraudulent activities. In general, insiders require their information to be private in order to ensure that their personal data is protected from illegal usage. Consequently, insider threat solutions should avoid the use of personal data as much as possible and should design a mechanism to protect this data from unauthorized access

(Yang et al., 2015). Therefore, there is a need to develop an insider threat solution that takes into consideration the changing nature of insiders while balancing their privacy when conducting workplace monitoring.

The complex nature of insider threat problems requires various approaches to address the changing human nature, social factors, organizational factors and privacy issues (Elmrabit et al., 2015; Hunker & Probst, 2011; Sanzgiri & Dasgupta, 2016).

This research proposes an insider threat prediction and prevention model based upon a comprehensive understanding of criminology while preserving the privacy of insiders and collecting current contextual information about insiders. The Fraud Diamond is used as a framework for this study, as it considers the basic tenets of crime as well as detection and prevention.

1.4 Research questions

The main research question is: How can approaches from criminology and computer science be integrated into a feasible model that will address the insider threat problem?

To answer the main research question, the research will answer the following sub-questions:

> RQ1: To what extent can the components of the Fraud Diamond be feasibly applied to address the insider threat problem?
>
> This question will be answered by studying the Fraud Diamond and mapping it to the insider threat problem, as it also has commonalities with other crimes. The application of each element of the Fraud Diamond in the insider threat domain will be discussed and included in the model. It will also be demonstrated by using prototypes.
>
> RQ2: To what extent can the physical and virtual contexts be used to predict an insider threat?

One of the problems in insider threat mitigation is collecting information about insiders that will be used for prediction and prevention. This research will investigate existing techniques to collect information about specifically related current contexts of insiders in order to collect usable information.

RQ3: To what extent can the privacy of insiders be preserved by an insider threat prevention and prediction model?

This question will be answered by studying the current limitations of insider prediction and prevention models in preserving the privacy of insiders so as to propose a new model that will balance the privacy of insiders, based on effecting privacy-preserving techniques.

RQ4: To what extent is the proposed model effective in preventing and detecting insider threats?

This question will be addressed by demonstrating the model, using a prototype and also by presenting both the model and the prototype for expert evaluation.

1.5 Research objectives

In this section, the research objectives including a general objective and other specific objectives will be discussed.

1.5.1 General objective

The general objective of the research is to propose a privacy-preserving, context-aware, insider threat prevention and prediction model, based on a comprehensive understanding of crime prevention theories.

1.5.2 Specific objectives

To achieve the general objective, the study attempts to address the following specific objectives:

- Investigate existing approaches from criminology and computer science to address gaps in current insider threat and prediction models.
- Propose a novel insider threat prevention and prediction model, based on a comprehensive understanding of the criminology theory.
- Develop a prototype that will simulate the model to be used to demonstrate concepts in the model.
- Undertake preliminary model testing involving selected experts from the field to collect feedback about the model (first iteration).
- Refine the model and the prototype, based on feedback collected from experts in the first iteration.
- Evaluate the refined model to collect second-round feedback from experts (second iteration).
- Revise the model, based on expert opinions from the second iteration.

1.6 Significance of the study

This study is expected to produce research evidence as to the applicability of integrated approaches, based on the understanding of the criminology theory and computer science to mitigate insider threat problems. The research specifically investigates the application of the Fraud Diamond to predict and prevent insider threats, as Fraud Diamond elements have been used effectively by other researchers to mitigate threats to both cyber and physical crimes (Brown et al., 2013; Kandias et al., 2010; Skousen, Smith & Wright, 2009).

The study also demonstrates that insider threat mitigation strategies can be developed while protecting the privacy of insiders while conducting workplace monitoring. Organizations can also use the proposed model as a framework to develop or acquire any information security system to address the problem of insider threats.

This research may also be helpful to organizations in deciding on a security system investment.

Finally, this research can also be used by other researchers as a framework to further investigate the problem of insider threats while preserving the privacy of insiders.

1.7 Scope of the study

In this section, both the scope of the research and the limitations of the study will be discussed.

1.7.1 Boundaries

This research focuses only on insider threats that are conducted by individuals in the cyber domain and does not assess threats that are done in groups, which is called collusion threats. The main purpose of this study is to address the insider threat problem, based on reviewing available literature in the field of insider threats and related areas as well as to collect expert opinions for information security professionals.

1.7.2 Limitations of the study

The researcher used purposive sampling to select a panel of experts based on studying their qualifications and experience in information security as stated in their LinkedIn profiles that may have a bias against the study. The study may also be biased by the expertise of the panel members. The other limitation with the sample is some of the selected experts were not willing to participate in this study specifically; the researcher was unable to recruit information security auditors to participate in the panel. The research used the same participants in the first and second iterations, which may have biased the study; however, it is imperative to utilize the same participants in order to assess refinements to the model.

The evaluation process was facilitated by the researcher, which may also be considered a bias against the study. However, to minimize the bias, the confidentiality of participants was guaranteed and pseudonyms were used to ensure that the identity of the participants would be kept confidential.

The model is evaluated based on a pilot application (prototype), simulation and expert reviews. However, there are other evaluation techniques in design science research such as laboratory experiments and field experiments (Österle, Becker, Frank, Hess, Karagiannis, Krcmar, Loos, Mertens, Oberweis and Sinz, 2011). This research study did not implement the techniques of laboratory and field experiments due to resource limitations, however, prototype and simulation techniques were used for evaluation.

1.8 Research design and methodology

The design science research approach is used to produce an artefact or design by studying the existing artefacts and developing a model along with validating the model by using demonstration (Peffers, Tuunanen, Gengler, Rossi, Hui, Virtanen & Bragge, 2006). Design science is highly applicable as a methodology to the information systems domain (Adomavicius, Bockstedt, Gupta & Kauffman, 2008; Bichler, 2006; Peffers et al., 2006, Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007; Von Alan, March, Park & Ram, 2004). This study adopts a design science research approach as proposed by Peffers et al. (2007). The research methodology adopted for this research is also evaluated, based on seven design science research guidelines proposed by Hevner, March, Park & Ram (2004). The study has adopted the basic principles proposed by Österle et al. (2011) that information systems research that is based on design science research should conform in order to evaluate the proposed model.

Once the model was developed based on extant research and related areas based on principles of design science research, it was presented to a panel of experts selected by using purposive sampling to collect their feedback on two iterations. The participants completed online questionnaires to provide their feedback after reviewing the proposed model as well as the prototype. Their feedback was used to refine the model and the prototype within two iterations, based on the guidelines of design science research.

Finally, qualitative comments of the participants were categorized and listed manually in the form of frequency counts as well as bar and pie charts, followed by a discussion for both iterations.

1.9 Structure of the thesis

The thesis is organized into eight chapters comprising the Introduction, Insider threat problem, Conceptual framework, Methodology, Privacy-preserving, Context-aware insider prediction and Prevention model (PPCAIPP), Evaluation: Cycle I, Evaluation: Cycle II and Conclusions and future research. This chapter offers an introduction to the thesis.

The second chapter discusses the insider threat problem, approaches to mitigate insider threats and current insider threat prevention and detection models.

The third chapter presents the conceptual framework used for the model proposed in this research study, including the Fraud Diamond, situational crime prevention, context-aware systems and privacy-preserving techniques.

The fourth chapter discusses the methodology employed for this research, specifically the design science research adopted for this study.

The fifth chapter presents the model proposed in this research, namely a **P**rivacy-**P**reserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**rediction and **P**revention Model designated PPCAITPP, including the derivation of the model and each component of the model.

The sixth chapter reports the results of the evaluation for the first iteration carried out in consultation with the panel of experts.

The seventh chapter discusses the results of the evaluation for the second iteration.

Finally, chapter eight concludes with the recommendations drawn from the findings of the study and future research avenues.

1.10 Conclusion

Insider threat problems are complex, as they are committed by individuals who are trusted and who have provided credentials to access information resources of the organization. As insiders are people, they have different motivations and dynamic behaviours for committing crime, and these make it challenging to predict and prevent insider threats. Another challenge in addressing an insider threat problem is that insiders expect reasonable privacy at work. Workplace monitoring to mitigate insider threats needs to balance privacy issues otherwise employees may become frustrated and their productivity may be affected negatively. Thus, the insider threat problem requires a solution that will address the human nature of insiders who have access credentials to balance their privacy.

This research proposes an insider threat prediction and prevention model, based on the understanding of the criminology theory, mainly the Fraud Diamond, to address insider threats, considering the multidimensionality of the insiders while preserving their privacy.

Organizations can use this model to help them in developing their information security strategy and it can also be used by other researchers to understand the insider threat problem and investigate the problem further.

The next chapter will discuss the insider threat problem in detail and current approaches to address insider threats will also be discussed.

CHAPTER TWO

THE INSIDER THREAT PROBLEM

2.1 Introduction

In this chapter, the problem of insider threats will be discussed, reviewing literature in the field, as it is one of the requirements for design research to build on prior research (Peffers et al., 2007). The chapter discusses the insider threat problem, including its definition, the types of threats, the types of insider crimes and the approaches to the insider threat domain The chapter includes a discussion of the current models for insider threat prediction and prevention in order to identify gaps in the extant literature. Finally, the chapter discusses the motivations to develop the model for this research, based on the discussion on the limitations of the current models to mitigate insider threats.

2.2 Insider Threat

In this section, the definition of the insider threat will be presented, followed by a discussion of the various categories of attacks and insider crime. Finally, the various approaches to contain insider threats will be discussed.

2.2.1 Definition of 'insider threat'

As the insider threat lacks a common definition, this section will review the various definitions as identified in the literature. The most common understanding of the term 'insider' is illustrated in the definition given by Anderson, Bozek, Longstaff, Meitzler and Skroch (2000). They state that an insider is "an authorized user who performs unauthorized actions that result in loss of control of computational resources" (p.21). According to this definition, an insider threat is a trusted and authorised user who uses their access to commit maleficence.

There are other definitions that emphasize the intention behind a malicious act. Some users may intentionally abuse computational resources to gain some advantage like financial gain while others may be involved in malicious activities accidentally without intention. Cappelli, Moore, Trzeciak and Shimeall (2009) postulate that a "malicious insider is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems" (p.5).

While other definitions include non-human actors in addition to the people involved in malicious acts. Walker (2008) defined an 'insider' as a "current or former human or non-human actor who intentionally exceeded or misused an authorized level of access to CIS, networks, systems, services, resources or data in a manner that targeted a specific human or non-human actor or who affected the confidentiality, integrity or availability of the nation's data, systems and/or daily operations" (p.226).

Some definitions even include insider types and the motivation behind committing a crime. One example of such a definition is suggested by the Centre for the Protection of National Infrastructure (CPNI): "Insiders can take a variety of forms including disaffected staff, single-issue groups (such as animal rights activists), journalists, commercial competitors, terrorists or hostile intelligence service agents. Their motivations are similarly varied and can range from political or religious ideologies to revenge, status, financial gain, and coercion" (Centre for the Protection of National Infrastructure, 2008, p.9).

The insider workshop that was held at Dagstuhl in 2008 derived a definition, emphasizing authorization and trust: "An insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure" (Probst, Hunker, Gollmann & Bishop, 2008, p.5). In their definition, empowering a user with providing a right to access and deciding on computational resources implies that the organization trusts the individual, however, the level of trust will vary from organization to organization, depending on the level of monitoring and control policies that are implemented.

Sanzgiri and Dasgupta (2016) define an insider as “a malicious user who has or at some time had authorization to an organization’s resources and involved in any one of the following activities:

- Unauthorized extraction, exfiltration of data
- Tampering with data or resources of an organization
- Destruction or deletion of critical data and assets
- Eavesdropping and packet sniffing with ill intent
- Impersonation of other users via social engineering” (p.25)

The above definition focuses on authorization as well as involvement in criminal activities.

This research adopts a definition by Elmrabit et al. (2015). The authors define an ‘insider threat’ as

(a) “Any malicious activities that cause damage to an organization’s IT and network infrastructure, applications, or services” (p.1);

(b) “On the part of an employee (current or former), contractor, subcontractor, supplier, or trusted business partner” (p.1);

(c) “Who has or has had authorized access to the organization’s IT assets” (p.1);

(d) And poses a significant negative impact on the information security elements (confidentiality, integrity, and availability) of the organization” (p.1). This comprehensive definition considers authorization, insider types and also the attack nature that may be carried out.

2.2.2 Categories of insider threats or attacks

There are different types of attacks committed by insiders. The most common types of attacks, as reported in the literature, are misuse of access, defence bypass, and access

control failure (Elmrabit et al., 2015; Hunker & Probst, 2011; Sanzgiri & Dasgupta, 2016; Stolfo, Bellovin, Hershkop, Keromytis, Sinclair & Smith, 2008). The mitigation approach should also be different for each type of attack. The types of attacks are discussed below.

2.2.2.1 Misuse of access

In this type of attack, the insider misuses the legitimate access granted by the organization for illegal acts. Since insiders are using authorized accounts, it is difficult to tackle the use of technical defences unless the usage patterns of the insiders are monitored as with their file access behaviour, download patterns, and logging patterns. For instance, a library circulation attendant may have been authorized to check books in and out to his or her pattern with legitimate access credentials. The attendant may allow the check-in of books without the patron returning the borrowed books. The fraud may not be noticed within a short time until the library undertakes a physical inventory of its books.

2.2.2.2 Defence bypass

Most of the organizations have a technical defence like a firewall to protect their systems from external access but insiders are already within that firewall and it is easy for them to attack the system. Insiders also have legitimate credentials so that they can log in to the system and abuse the system by means of their authorized activities. For this attack, organizations may design detection systems that can identify anomalous behaviour or actual attacks on nominally-protected systems.

2.2.2.3 Access control failure

In this type of attack, the problem lies with the organization’s authentication system which may allow erroneous access details due to technical problems in the configuration. The insiders may attempt to access the system since they have proper authorization. Organizations should periodically monitor their systems to check any types of access control failure and they can also implement a technical solution to distinguish any anomalous behaviour from normal activities.

2.2.3 Categories of insider crimes

There are three common types of crime that insiders commit, namely information technology (IT) sabotage, theft of intellectual property (IP), and fraud, as reported in the literature (Agrafiotis, Erola, Happa, Goldsmith & Creese, 2016; Cappelli, Moore & Trzeciak, 2012; Elmrabit et al., 2015). The three categories of insider crimes will be discussed below.

2.2.3.1 IT sabotage

IT sabotage refers to a case where insiders exploit information technology to harm an individual or an organization directly. Every organization that uses IT to manage its activities is in danger of facing IT sabotage threats. As per the database collected by Computer Emergency Response Team (CERT), in one of the cases an insider destroyed a database of research works on cancer which was never recovered (Cappelli et al., 2012). In another case, critical data of a financial institution was deleted when all servers of the organization were affected by a logic bomb and there was no data for operation when the institution opened for business in the morning.

According to Cappelli et al. (2012) and Elmrabit et al. (2015), these types of attacks are committed by technically sophisticated IT professionals, as system administrators suggest both technical and non-technical solutions to mitigate IT sabotage (Cappelli et al., 2012; Elmrabit et al., 2015; Sanzgiri & Dasgupta, 2016).

A study conducted by Keeney, Kowalski, Cappelli, Moore, Shimeall and Rogers (2005) affirms that “40% of insiders who have committed IT sabotage have a criminal history, including being involved in violent offenses, alcohol or drug-related offenses and non-financial/fraud-related theft offenses” (p.12). Another suggestion by the authors is that clearly communicating organizational IS security policies are important so that employees will not commit a crime unknowingly, and hence eliminating any excuse for fraudulent behaviour. They also suggest that supervisors should be trained in security

precautions so that they will clearly understand any deviation from normal behaviour to take the necessary action such as sanctioning a potential insider.

One of the technical solutions suggested by the authors is to monitor and eliminate any unknown access paths such as shared accounts and logic bombs and to disable the paths once they are known. Monitoring any change in source codes of the organizational information system is also important. It is very important to secure system logs, as the logs show the activities of the insider. It is suggested that organizations take measures to protect electronic back-ups, as the back-ups may be targeted by insiders and used to recover a system that has been attacked by IT sabotage.

2.2.3.2 Theft of intellectual property (IP)

Theft of intellectual property refers to attempts by insiders to steal the intangible assets created and owned by the organization that is very important to achieve its mission (Cappelli et al., 2012).

Cappelli et al. (2012) compiled a database in which they show previous incidents with stolen intangible assets through theft of IP, including:

- Proprietary software/source code
- Business plans, proposal, and strategic plans
- Customer information
- Product information (designs, formulas, schematics)

In one of the incidents compiled by CERT, an insider stole trade secrets worth $40 million by copying them to removable media. She later used these secrets to start her own business with her husband. In another case, an engineer who was working for a high-tech company stole trade secrets from his organization and initiated similar businesses by acquiring funding from foreign organizations.

According to Cappelli et al. (2012), most of the insiders stole IP not to gain financial advantage by selling it to external parties but rather to gain business advantage to either

start their own businesses or to use it for their work in another organization or to start businesses by partnering with foreign governments and companies.

An interesting finding by Cappelli et al. (2012) is that all of the intellectual property (IP) theft cases were committed not by IT staff like system administrators as most people would assume; rather it was committed by other employees such as scientists, engineers, programmers or salespeople. These insiders committed the crimes by using their authorized credentials and during normal working hours, which makes it challenging to tackle. Cappelli et al. (2012) suggest organizations adopt technical solutions like "digital watermarking, digital rights management, and data loss prevention systems to prevent the problem from occurring" (p.352). It is also suggested that employees who are leaving the organization should be monitored, as most of the cases concerning IP theft were committed by such employees (Cappelli et al, 2012).

2.2.3.3 Insider fraud

Insider fraud, as defined by Weiland, Moore, Cappelli, Trzeciak & Spooner (2010) "is an insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or the theft of information that leads to an identity crime (identity theft, credit card fraud)" (p.8). This crime will seriously affect the organization as it may lose its customers' trust; for instance, if the credit card number of a customer is stolen.

In one instance, as compiled by CERT databases, a customer service representative who was responsible for processing health insurance claims intentionally changed the address of medical care providers who rarely filed claims. He then laid a claim on behalf of the medical care providers and later collected $20 million from his fraudulent activities.

In another case, a database administrator who was responsible for maintaining the customer records of an insurance company downloaded the personal information of customers, including their credit card details by using removable media in an attempt to take revenge on his organization. He complained that he was not fairly paid for his work.

He also planned on using the database to make money by selling it to online fraudsters. As revenge, he posted the credit card details of the employees in an online newsgroup of fraudsters and also encouraged them to abuse the credit cards. He carried out these fraudulent activities for more than two years until an undercover agent who approached him as a buyer of credit cards caught him.

Like theft of intellectual property, current employees commit this type of fraud while they are performing their normal activities during normal office hours. They compromise their authorized credentials to abuse the system to gain personal benefits rather than achieving the organizational mission. However; the difference between theft of IP and IT sabotage is that insider fraud is committed mostly by lower-level employees and not the middle and upper-level employees. The fraudsters are mainly motivated to gain financial benefits (Cappelli et al., 2012). Another feature of insider crimes is that insider fraud takes a long time to occur. According to the CERT databases, insider fraudulent activities take about fifteen months on average to occur (Cappelli et al., 2012).

With respect to mitigation strategies, Cappelli et al. (2012) suggests that there is a need to focus on prevention, detection and response approach, as with other insider crimes. The preventive approaches should focus on reducing opportunities for crimes to be carried out. For instance, an employee with a criminal history is likely to commit the same crime to his current employees. Thus, there is a need to check the backgrounds of employees before making a decision to hire the employee.

Insider fraud can be detected in two ways, namely by using internal controls and involving external parties' investigators from law enforcement. The organization may detect insiders in the planning stage, either during insider recruitment or through online execution. In serious fraud cases where external fraudsters are involved, they may cooperate with external law enforcement agencies for undermining the investigation (Cappelli et al., 2012).

2.24 Insider threat mitigation

The complex nature of insider threat problems requires a variety of approaches depending on the nature of the types of the insider attacks and the organizational contexts. There are three major approaches for monitoring and mitigating insider threats namely technical, sociological and socio-technical as suggested in the literature (Hunker & Probst, 2011; Elmrabit & Yang, 2015; Sanzgiri & Dasgupta, 2016; Agrafiotis et al., 2016)

2.2.4.1 Technical Approaches

2.2.4.1a Intrusion detection systems

Intrusion detection systems(IDS) is mainly borrowed from solutions from external attacks and focus on identifying any malicious activity on a computer network and system violating Information policy of the organization such as inappropriate access or accessing sensitive information without authorization (Brancik, 2007). There are two major strategies IDS approaches which are Misuse detection and Anomaly detection. The former focuses on monitoring any usage behaviour that deviates from standard rules in the organization and is considered a misuse (Magklaras & Furnell, 2010), while the latter usually uses machine-learning approaches to learn normal behaviour of users so as to detect any deviation from normal behaviour (Hori, Nishide & Sakurai, 2011).

Li, Meng and Horace (2017) designed an IDS based on supervised machine-learning approaches to detect insider threats. Their model was assisted by an expert to determine the trustworthiness of a specific user to train a model of trusted users and later to be used to evaluate any new instances. Meng, Li, Xiang and Choo (2017) also implemented an IDS system based on machine-learning approaches to protect medical smartphone networks from insider threats. Their implementation was based on a statistical machine-learning algorithm called Bayesian inference in order to predict the probability of malicious activities, and their model was found effective based on their evaluation.

Wang, Yang, Liu and Li (2011) also used a machine-learning approach based on a Bayesian learning model to develop a process model for normal insider behaviour so as to detect any malicious activity that deviates from normal behaviour. Ambre and Shekokar (2015) proposed an IDS system based on monitoring log files of a user's activity to identify the probability level of malicious activities in comparison with a normal log file in combination with event correlation.

IDS systems are often considered to be time-consuming and overly reliant on copious amounts of data and further insider data is highly sensitive and confidential (Stolfo et al.,2008). IDS systems also suffer from false positives, which may negatively affect productivity (Claycomb & Nicoll, 2012).

2.4.4.1b Access control

Insiders are authorized to use the information system of the organization and access control approaches argue that if there are effective access control policy mechanisms in the organization, the risk of attack by insiders will be minimized (Babu & Bhanu, 2015)**.** Several other access control mechanisms mainly focus on controlling the authentication of authorized insiders. Authentication focuses on correctly identifying an insider based on mechanisms such as passwords, multilevel authentication schemes, biometrics etc. while authorization ensures that insiders have proper permission for specific access to information resources (Sinclair & Smith, 2008)**.**

Traditionally, access control systems have been based on role-based access control which gives permissions to users as far as they are authorized to do so (Safa, Maple, Watson & Von, 2018). However, some researchers argue that there is a need to consider the risk of the level of specific information resources and the trust level of the users when implementing authentication and authorization systems such as role-based access control mechanisms (Babu & Bhanu, 2015**.**

Several other research works also integrated considering risk level specific information resources on access control system so that the access control for high-risk resources will be limited. (Bishop et al., 2010; Baracaldo & Joshi, 2012; Peisert & Bishop, 2013). Almehmadi and El-Khatib (2017) proposed another variable to consider in access control systems which is the intentions of the insiders when accessing the information resources of the organization which is called intent-based access control.

Access control systems are still criticized for the risk of exposure to insider attacks as several statistics show that users are turning into malicious insiders after they are being considered legitimate and trusted by the access control system (Almehmadi & El-Khatib, 2017). Access control systems are also critic beset by their high false positives as the level of trust that is given to insiders to access resources might not be always appropriate and sometimes high-risk insiders might be given authorization to critical information (Bishop et al., 2010)**.**

2.2.4.1c Honeypot

Spitzner (2003) defined a honeypot as a "… security resource whose value lies in being probed, attacked or compromised" (p.37). Honeypots are an effective detection tool for an insider threat with low false positive rates as it only focuses on containing an insider threat (Bowen, Salem, Hershkop, Keromytis, & Stolfo, 2009). A number of studies have been conducted on using honeypots to detect the insider threat (Brown et al., 2009; McGrew, 2006; Spitzner, 2003; Padayachee, 2015). Cenys, Rainys, Radvilavius and Gotanin (2005) have developed three honeytoken modules and incorporated it into the DBMS Oracle 9i Enterprise Edition for the purpose of trapping intruders who attempt to attack information systems. Padayachee (2015) employed honeypots to lure insiders into maleficence and then her model intervened to remove any justifications/rationalizations the insider might use to attack the target by using the neutralization mitigation technique. Brown et al. (2009) have also used honeypots by producing a decoy document to detect any malicious activity by means of monitoring the interaction of insiders with the decoy document.

There is an issue of privacy when implementing honeypots as it is used to detect a malicious insider without the explicit knowledge of the aforementioned insider. There is also a need to check the legal environment of the organizations as it may be illegal in some cases to deploy honeypots without the explicit knowledge of employees (Brown et al. 2009).

2.2.4.1d Monitoring

Some organizations monitor both the online (Hansen & Atkins, 1993; Prewett & James, 2004) and offline (Sah, 2002) activities of their employees to detect any risk of insider threats (Ambre & Shekokar, 2015)**.** Nguyen, Reiher, and Kuenning (2003) proposed monitoring employees based on call analysis. Ambre and Shekokar (2015) proposed a model for monitoring insider's activities based on log analysis with event correlation. Brown et al. (2013) recommended monitoring electronic communications of insiders to detect any malicious activities. Grigori et al. (2004) proposed an analysis of business processes of employees to detect any suspicious activities by insiders. Gritzalis, Stavrou, Kandias and Stergiopoulos (2014) proposed a monitoring model which is based on analysis of social media communications of insiders to detect any behaviour attributed to insider threats. Suh and Yim (2018) recommended a use electroencephalogram (EEG) monitoring to detect any brainwave signals that might indicate the risk of an insider threat.

Monitoring approaches especially that is based on electronic communications in E-mail and social media interactions are highly criticized for abusing the privacy of insiders and also there are a number of ethical issues that are raised with such approaches (Fazekas, 2004; Gritzalis et al., 2014).

2.2.4.1e Continuous auditing

Continuous Auditing is defined as "a methodology that enables independent auditors to provide written assurance on a subject matter, for which an entity's management is responsible, using a series of auditors' reports issued virtually simultaneously with, or a

short period of time after, the occurrence of events underlying the subject matter" (CICA, 1999, p.1). The problem with traditional external auditing techniques are audit information is collected after some period of time which makes it difficult to correct any fraudulent activities; however, continuous monitoring collects audit information in real-time environments using automated tools (Vasarhelyi, Halper & Ezawa, 1991; Hansen & Hill, 1989; Chiu, Liu & Vasarhelyi, 2018). Thomas and Marathe (2012) proposed the use of continuous auditing based on stochastic game theory to detect an insider by computing the expected behaviour of a fraudster in a transaction system. Montelibano and Moore (2012) also recommended the use of continuous auditing to detect insider threat and make corrective measures timely.

Continuous auditing is criticized by its high resource requirements in organizing automated tools to do auditing at run time and also the resources required to manage the auditing system continuously (Rikhardsson & Dull, 2016). Due to its resource requirements, it is mainly used by large organizations and it is not common in small organizations (Rikhardsson & Dull, 2016).

2.2.4.1f Policy-based mechanisms

Policy-based mitigation strategies for insider threats are also considered as major technical approaches to address the insider threat problem (Team, 2000; Yu, Fayaz, Collins, Sekar & Seshan, 2017). Policies help organizations to limit what is permissible and non-permissible behaviours according to which insiders need to behave while accessing and using information resources of the organization, supported by policy languages to deal specifically with technical issues (Probst, Hunker, Gollmann & Bishop, 2010)**.** Policies are also implemented to manage access controls using tools like Policy Decision Points (PDPs) along with Policy Enforcement Points (PEPs) as applied by Ali, Ahmed, Ilyas and Küng (2017) to manage access control in a relational database in a cloud computing environment.

The application of the policy-based approach to address insider threats has also been found effective in health-focused organizations (Ahmed, Latif, Latif, Abbas & Khan, 2018). Some studies have also been done to provide solutions to any policy violations, for instance, Kammüller and Probst (2013) recommended a vector model to identify situations that will lead to policy violations. There are also other studies conducted based on policy invalidation to avoid any policy violations by exploring attack possibilities (Kammüller & Probst, 2013, 2014, 2017).

Policy-based approaches in themselves are not taken as holistic mechanisms to address insider threats, as insiders might still commit a crime, violating the policy, especially as insiders can be deceived by social engineering techniques (Kammüller & Probst, 2017; Greitzer et al., 2014). Technical policies are also criticized for their limitations to predict the unexpected behaviour of insiders, and it is included as part of the policy to be applicable in different contexts (Probst et al., 2010). A common criticism levelled at policy-based approaches is that they are not updated frequently and that they are not updatable based on the dynamic nature of insiders (Probst et al., 2010; Kammüller & Probst, 2017).

2.2.4.2 Social sciences- and criminology-based approaches

Purely technical approaches cannot fully address the insider threat problem as the problem involves the human element. The human element is dynamic and difficult to predict. Consequently, several studies suggest that the human element should given due consideration in addition to the technical concerns (Hinde, 2003; Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005; Krombholz, Hobel, Huber & Weippl, 2015; Safa et al., 2015; Safa, Maple, Watson, & Von Solms, 2018). The following section discusses approaches borrowed from psychology, behavioural studies and criminology to consider human factors from an insider threat perspective.

2.2.4.2a Psychological/behavioural and social approaches

Various studies recommended that the behaviour of insiders should be studied to design and implement security solutions as human factors are crucial in addressing the insider threat problem. (AlHogail, 2015; Boss, Galletta, Lowry, Moody, & Polak, 2015; Hsu, Shih, Hung & Lowry, 2015; Posey, Roberts, Lowry, Bennett, & Courtney, 2013; Vance, Lowry, & Eggett, 2015; Krombholz et al. 2015; Safa et al., 205). Some studies (see Fagade and Tryfonas (2016) and Hausawi (2016)) have attempted to investigate the positive and negative behaviours that might trigger an insider threat, in order to identify future insider threats. Greitzer, Kangas, Noonan, Dalton and Hohimer (2012) and Greitzer and Frincke (2010) also studied the common behaviour of insiders based on previous insider threat scenarios as well as with discussions with security professionals and human resource experts. Cappelli et al. (2008) and Nurse et al. (2014) proposed a framework to identify the behaviours of insiders based on a case study of previous insider threat incidences. Niihara, Yamada, and Kikuchi (2017) also studied the relationship between sharing credentials behaviours and insider threat and found that those insiders who share credentials are at high risk for committing a crime. Burns, Posey, Roberts and Lowry (2017) proposed a different perspective to deal with the behaviour of insiders based on positive psychology, which argues that rather than focusing on negative behaviours which result in insider threat it is better to focus on fixing what is a right behaviour to prevent future insider crime. Hills and Anjali (2017) recommended the application of Nudge theory (Vallgårda, 2012) to address insider threat which argues that we should work on improving the organizational system that will provide positive choices for insiders so that their behaviours will be more inclined to keep the information security policy of the organizations avoiding any violations.

Some studies argue that organizations should not only focus on considering the individual behaviours of insiders but also their interactions in a social environment (Baracaldo, Palanisamy & Joshi, 2017; Kandias et al., 2013; Ali, Ahmed, Ilyas & Küng, 2017). Ali et al. (2017) included the investigation of insider's social interaction as parts of their framework to predict and detect insider threats. Baracaldo et al. (2017) also proposed a

framework that is to be used to mitigate insider threat based on analysis of the social interaction of insiders.

Psychological or behavioural and social approaches are still challenging to implement due to the unpredictable nature of insiders and also the dynamism involved in social interactions (Theoharidou et al., 2005; Workman, Bommer & Straub, 2008). Privacy and ethical issues are raised in this approach as monitoring the behaviours of insiders and their social interactions affect their privacy and there is a need to balance privacy when implementing such approaches (Gritzalis et al., 2014; Fazekas et al., 2004; Suh& Yim, 2018).

2.2.4.2b Criminology

Various criminology theories, which have been used to detect and prevent crimes in the physical domain, have also been applied to the insider threat problem (Hollinger, 1993; Neumann, 1999; Parker, 1998; Tuglular, 2000; Willison, 2004; Theoharidou, 2005; Padayachee, 2013, 2015). Straub and Welke (1998) investigated the application of General Deterrence Theory in computer crime with the hypothesis that insiders make decisions based on maximizing their benefit and minimizing their loss in committing a crime. Lee, Lee and Yoo (2004) proposed the application of Social Bond Theory to the insider threat problem with the justifications that social bonds can be increased to reduce computer crime by implementing an effective security policy, security system and creating awareness on the values of the policy. Lee and Lee (2002) and Skinner and Fream (1997) recommended the use of Social Learning theory in information security domain justifying that insiders can be influenced positively by their colleagues not to be involved in malicious acts. Padayachee (2013) and Padayachee (2015b) provides a conceptual framework based on situational crime prevention theory (SCP) to mitigate the insider threat from an opportunity-based perspective. Padayachee (2015a) also proposes an insider threat neutralization mitigation model, based on the SCP theory, the neutralization theory, and the cognitive dissonance theory to mitigate insider threats. Me and Spagnoletti (2005) have also used the application of SCP to specific insider threat

crimes such as online pedo-pornography while Reyns (2010) considered the theory towards cyberstalking. Beebe and Rao (2005) have made a digital analogy for 16 opportunity-reducing techniques of SCP, as proposed by Clark (1997).

The effectiveness of criminology theories in insider threat is being investigated and it has not been fully tested and requires further studies (Ali et al., 2017)**.** The issue of privacy and ethics should also be taken into consideration when applying criminology theories as some of some of these theories are based on a study of behaviours of insiders which might abuse the privacy of insiders.

2.2.4.3 Integrated approaches

The insider threat problem is a complex problem with various indicators including technological, behavioural, psychological, organizational and legal factors which requires a holistic approach to integrate various solutions in order to mitigate malicious insiders effectively (Schultz, 2002; Greitzer, Frincke, & Zabriskie, 2012; Fagade, Spyridopoulos, Albishry, & Tryfonas, 2017; Nurse et al. 2004). Some researchers attempted to add psychological/behavioural perspective in technical approaches like intrusion detection system so as to improve the performance of insider threat detection system (Magklaras & Furnell, 2001; Greitzer & Hohimer, 2011; Legg, Buckley, Goldsmith & Creese, 2015). Babu and Bhanu (2015) also proposed a model which included the assessment of the behaviour of insiders using a keystroke mechanism with the risk-based access control system. Fagade et al. (2004) integrated studying the behaviour of insiders using planned behaviour theory combining it with log analysis and social media footprints. Boender, Ivanova, Kammüller and Primiero (2014) also attempted to integrate technical and social approaches by proposing the representation of insider behaviour using a sociological approach and higher order logic from computer science. Arulampalam, Maskell, Gordon and Clapp (2002) also attempted to use the Bayesian network with an assessment of the behaviour of networks to predict insiders based on text and social media data.

Nurse et al. (2014) proposed a general framework to characterize insiders including various factors which includes technological, behavioural/psychological, and human factors to understand the complete picture of insiders. Ali et al. (2017) also proposed a framework to mitigate insiders covering technical behavioural and human factors. Kandias et al. (2010) model to predict insider threats based on technical, behavioural, human factors and criminology theory. The model proposed in this research is also an integrated approach, which includes technical, behavioural and criminology perspectives. The integrated model proposed in this research will be discussed in detail in chapter five.

2.3 Extant Insider Threat Prevention and Prediction Models

The research community in the information systems security domain has attempted to address the insider threat problem by proposing various approaches and models. The research contributions start with conceptualizing the insider problem so that there will be a common understanding among researchers (Hunker & Probst, 2011).

Research has been conducted to analyse the psychological characteristics of insiders in order to understand the human elements related to insider threats (Bishop, Conboy, Phan, Simidchieva, Avrunin, Clarke, Osterweil & Peisert, 2014; Brown, Watkins & Greitzer, 2013; Greitzer et al., 2013; Shaw & Stock, 2011). Some researchers also attempted to develop systems to detect any anomalies that might be a sign of insider threat behaviour (Salem & Stolfo, 2009; Thompson, 2004), while other authors attempted to develop models that could predict and/or prevent insider threats (Axelrad et al., 2013; Dimkov, Pieters, & Hartel, 2009; Dimkov, Pieters, & Hartel, 2010; Kandias et al., 2010; Probst & Hansen, 2008, 2009). Moreover, some research studies proposed an integrated model, which addresses the insider threat problem by integrating various models such as "honeypots, network level sensors, physical security logs, and models of insiders and pre-attack insiders" (p.4) (Maybury et al., 2005).

Most of the current insider threat models focus on addressing insider threats either from a technical perspective, excluding the human and organizational factors, or by focusing on the psychological characteristics of insiders; thus neglecting the technical perspective. However, the insider threat problem is a factor of all human behaviour, technical

controls, and organizational aspects. These elements require integrated solutions, which consider all elements, related to insider threats. This is one of the motivations for this research, namely to develop an integrated model, which addresses the human, the technical and the organizational factors.

One of the limitations of the current insider threat prediction and prevention model is that they do not consider the privacy of insiders. Employees expect to enjoy a reasonable amount of privacy in the workplace. If that is not the case, they may experience stress and frustration, which, in turn, may reduce their productivity levels (Brown, 1996; Dhillon & Moores, 2001). Some models monitor the e-mail and social media interaction of their employees and this practice may expose the personal data of the insiders to intruders (Brown, et al., 2013; Greitzer et al., 2013). Developing a model that will preserve the privacy of insiders is one of the major motivations for this research.

Another problem with current insider threat models is that their sources of data are not reliable. For instance, the model proposed by Kandias et al. (2010) is based on information collected from human resources data but it may not show the current behaviour of insiders. Typically the data collected may not be reliable, as insiders might provide false information. Proposing a model that automatically collects current and reliable information about insiders is another motivation for this research.

A further limitation of current insider threat models is that they focus on detecting and preventing insider threats but they exclude user education and awareness. These two aspects are crucial in preventing insiders from committing a crime as well as preventing future crime incidents. Developing a model that will educate any at-risk insider from committing a crime, based on the criminology theory is yet another motivation for this research.

This research proposes a privacy-preserving, insider threat prediction and prevention model, based on the Fraud Diamond integrating approaches from the fields of criminology, psychology, and computer science in an attempt to address the limitations of the current models.

2.4 Chapter summary

A basic introduction to the problem of insider threats has been discussed in this chapter (see section 2.2). The current approaches and models to mitigate insider threats have also been discussed (see section 2.24). The chapter also discussed the limitations of the current insider threat prediction and prevention models which includes the lack of integration of sociological and technical approaches, unreliable data and the infringement of privacy rights (see section 2.3).

Based on the limitations of the current models, this research is motivated to integrate approaches from psychology, criminology, and computer science to address human, technical, social and organizational factors related to insider threats (see section 2.3). The chapter has also discussed the research that is motivated to use a context-aware system to gather reliable and current information about insiders (see section 2.3). Privacy issues, as one of the limitations of the current models discussed in this chapter, and developing a privacy-preserving model are discussed as motivations for this research.

In the next chapter, the conceptual framework that is used to propose a new insider threat prediction and prevention model will be discussed.

CHAPTER THREE

CONCEPTUAL FRAMEWORK

3.1 Introduction

This chapter discusses the theories that are integrated into the model presented in this research. The model is adopted to address the limitations of the extant models to mitigate insider threat problems. The approaches are adopted from the disciplines of criminology and computer science, including the Fraud Diamond, situational crime prevention, neutralization mitigation, context-aware systems and privacy-preserving techniques. The discussion of the theories from extant research with its applications in the information security domain will be discussed in this chapter. The chapter also discusses what specific approaches from theories this research has adopted to develop the insider threat prediction and prevention model. The theories from the discipline of criminology form the basis for this research, as cybercrimes are crimes after all.

3.2 Fraud Diamond

In this section, the concepts of the Fraud Diamond will be discussed including its historical background, elements and its applications to the insider threat problem.

3.2.1 History of the fraud triangle

With an increased application of information technology in different business domains, the number of fraud occurrences has also increased with emerging new techniques to commit a fraudulent act that did not exist before (Mackevičius & Giriūnas, 2013). As a result, fraudsters are always seeking new techniques to commit fraud by analysing any loopholes in both internal and external environments of organizations. As a consequence of this challenge posed by fraudsters, organizations have been demanding auditors not only detect fraud that has been committed but also to prevent fraud before it occurs. According to Rezaee (2002), researchers and practitioners are advised to work together to

identify the causes of fraud being committed, the available techniques with which to commit a crime as well as the techniques to prevent the occurrence of fraud.

To address these challenges, Cressey (1953) conducted a study on blue-collar criminals to identify their reasons for committing their crimes. He found that three conditions needed to be present in order for fraud to occur. These conditions were pressure, opportunity, and rationalization. The authors represented their findings by using a fraud triangle, as shown in Figure 3.1. This model has been used extensively by various researchers and practitioners to analyse fraud.

However, the fraud triangle has also been criticized by some researchers. Kassem and Higson (2012), Anandarajan and Kleinman (2011), and Koerber and Neck (2006) argue that the fraud triangle does not satisfactorily analyse fraud, as it overlooks other factors such the capability and skills of criminals. According to Mackevičius and Giriūnas (2013), the fraud triangle also does not exhaustively analyse the motives behind the fraud. They argue that the motives are different, based on the factors such as gender and the degree of a favourable environment to commit a crime. Bressler and Bressler (2007) argue that not all employees who are under pressure have the opportunity to commit a crime and rationalize their criminal activities. The authors underline the fact that there must be another element which has the capability to induce a crime.

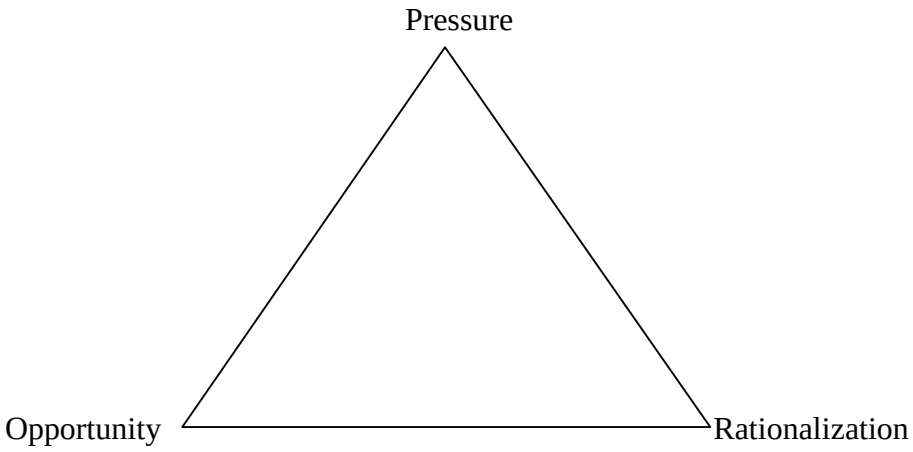

Figure 3.1 Fraud Triangle (adapted from Cressey, 1953)

3.2.2 Elements of the Fraud Diamond

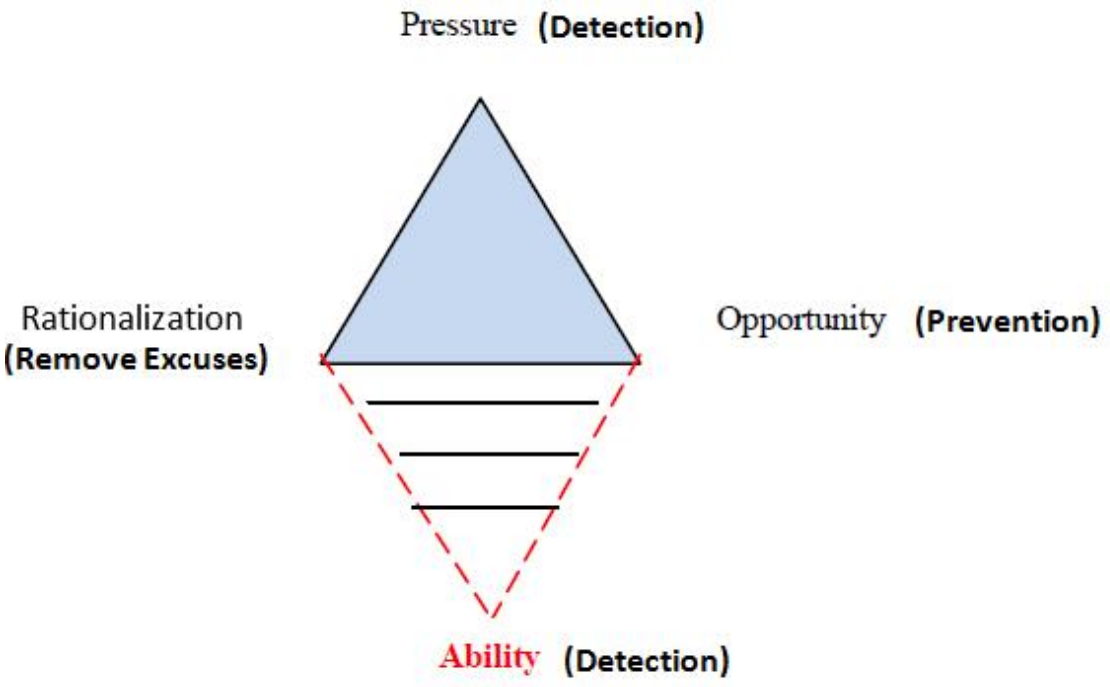

Figure 3.2 Fraud Diamond (adapted from Omar, Din and Faizal, 2010)[1]

Bressler and Bressler (2007) proposed the Fraud Diamond (see Figure 3.2), based on the idea that the fraud triangle is not inclusive of all factors to commit a crime. They argued that criminals do not only require pressure, opportunity, and rationalization but also the capability to commit a crime.

Albrecht, Wernz and Williams (1995) also argue that capability is a very important element, especially in crimes that are planned to be committed on a large scale. They also emphasize that only a person with capability can properly see a gap in an organizational environment, and is able to plan and execute an attack effectively.

The four elements of the Fraud Diamond, which are pressure, opportunity, rationalization, and capability, are discussed next.

[1] The ability and pressure elements of the Fraud Diamond is used to detect any insider risk. An opportunity is facilitated as a means to determine whether an insider that is under pressure with the requisite capability will take advantage of said opportunity. Remove excuse technique of situational crime prevention is used to remove any rationalizations that an insider may have to commit crime. The opportunity facilitation and rationalization technique is used a preventative measure.

3.2.2.1 Pressure

Pressure, also known as motivation, refers to the factors that drive employees to commit a crime. The pressure may be a real financial need such as covering medical costs or paying one's debt. It may also be related to a perceived need in which the insider has an urgent financial need but thinks that there may be future needs like acquiring materials for future use (Bressler & Bressler, 2007; Anandarajan & Kleinman, 2011; Mackevičius & Giriūnas, 2013). The pressures may perhaps not be financial in nature but they may be work-related. For instance, an employee may be tempted to commit a crime to cover-up faults that have occurred while doing his or her day-to-day activities (Mackevičius & Giriūnas, 2013). In some cases, addiction to drugs and gambling can be motivations for maleficence (Anandarajan & Kleinman, 2011). Pressure also occurs due to dissatisfaction with one's work environment, such as low wages and lack of promotion (Mackevičius & Giriūnas, 2013).

Mackevičius and Giriūnas (2013) classify pressures, based on their sources, which are internal and external. The classification is presented in Figure 3.3 .

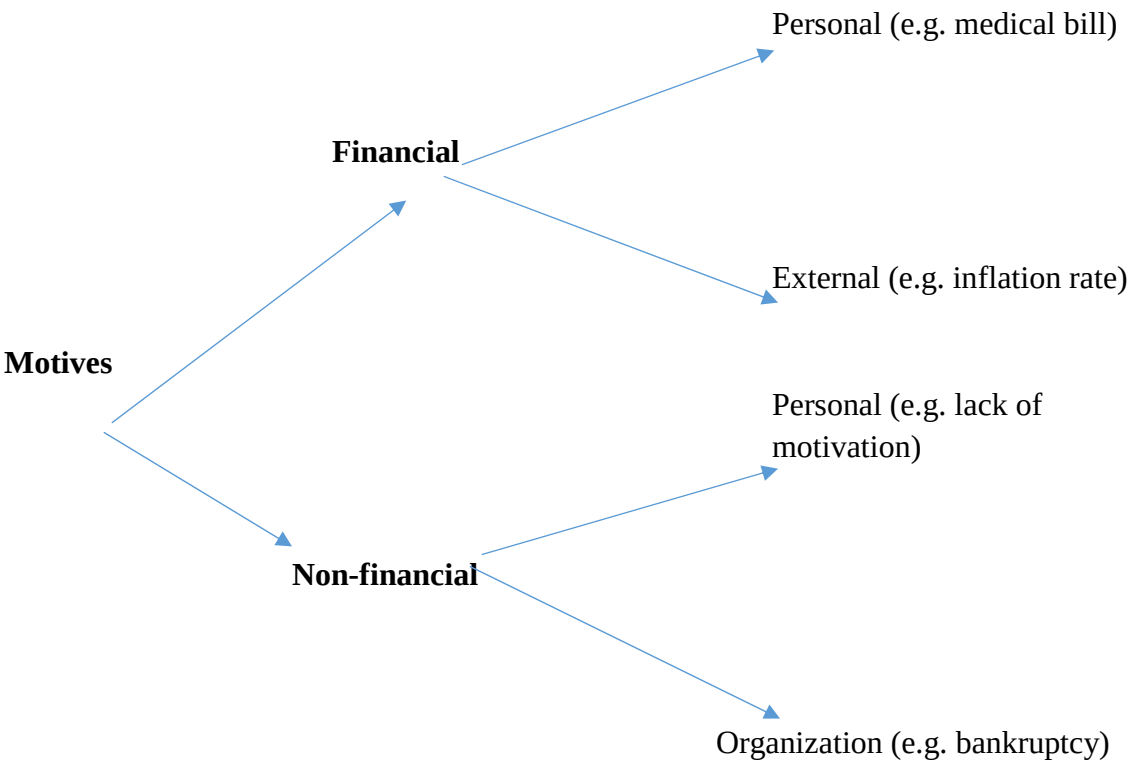

Figure 3.3 Classification of motives for committing fraud (adapted from Mackevičius and Giriūnas, 2013)

3.2.2.2 Opportunity

Opportunity refers to the ability to commit a fraudulent act resulting from favourable possibilities for fraud such as poor security control, management oversight, lack of periodic audits, etcetera (Bressler & Bressler, 2007; Anandarajan & Kleinman, 2011; Mackevičius & Giriūnas, 2013). Usually, criminals analyse the probability of being caught in their decision to commit a crime, which is an opportunity factor. Unless organizations establish standard procedures to detect fraud, fraudsters will be encouraged to engage in fraudulent activities. From the three elements, opportunity is the more tangible one, as organizations can institute processes, policies, and controls to discourage maleficence.

Mackevičius and Giriūnas (2013) have proposed a classification of opportunities that facilitate fraud to occur. They proposed seven groups of opportunities. These are:

1) The qualities of the managers in terms of honesty, capacity, and decision-making

2) The employees of the organization

3) The nature of the organizational structure

4) The financial performance and the productivity level of the organization

5) The activities of the organization as well as the industry in which the organization operates

6) The financial reporting and control systems, including accounting and auditing

7) External conditions such as government laws, competitors performance that affects the organization

The classification helps management to work on developing procedures and controls that will minimize favourable conditions for fraud. An example of conditions related to the qualities of the managers in terms of honesty, capacity, and decision-making may be having overambitious managers who set unrealistic goals to achieve. For conditions relating to the employees of the organization, lack of team spirit for common goals among employees may be considered as an obstacle. With regard to conditions related to the nature of the organizational structure, if there is no clear responsibility and limits for insiders it may lead to insider threat risk.

An example of conditions related to the financial performance and the productivity of the organization is contracted agreements with liabilities without assessing the capacity of the organization. With respect to conditions related to the activities of the organization as well as the industry in which the organization operates, making payments in cash for large portions of sales or purchases may be problematic. For conditions related to the financial reporting and control system, including accounting and auditing, an example could be the accounting procedures that are too complex, which makes it difficult for the organization to control these procedures. With regard to external conditions, changes in the labour market of the industry in which the organization operates may be another factor.

3.2.2.3 Rationalization

According to the Fraud Diamond, insiders need to justify to themselves their criminal actions to avoid guilt (Bressler & Bressler, 2007). For instance, an employee who thinks he/she is working hard and misses a promotion may say, “I deserve to commit fraud as revenge for not getting that promotion” when the employee justifies his or her fraudulent activities.

The following are common rationalizations that employees use to commit fraud (Mackevičius and Giriūnas, 2013):

- The fraudster justifies that he/she is committing the crime for the sake of saving a family member or loved one.
- The employee may be convinced that unless he/she commits the crime, he/she may lose the job, family, properties and so on.
- The fraudster may be frustrated and think there is no way out except committing the fraud.
- The employee may have huge debts and think that he/she should steal money to repay the debt.
- The fraudster may be dissatisfied with his/her employer due to factors such as low pay, lack of promotion and the like, and may thus justify his/her criminal activities as legitimate and rational.

Sykes and Matza (1957) suggest five techniques that organizations can use to remove any excuse/rationalization for their criminal actions. These techniques are denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and appeal to higher loyalties. Klockars (1974) and Minor (1981) include two more techniques, namely “the metaphor of the ledger” and “the defence of necessity” in addition to the five techniques proposed by Sykes and Matza (1957). Siponen and Vance (2010) have investigated the techniques suggested by Sykes and Matza (1957) and recommend all of the techniques except the denial of the victim, which should be implemented for information systems security solutions. They have also suggested that

the metaphor of the ledger and defence of necessity should be used as neutralization techniques in information systems security.

This research adopts the six techniques that have been proposed by Siponen and Vance (2013) for the information security domain. These techniques are discussed below.

Denial of responsibility

This technique refers to the justification that insiders avoid taking responsibility for their criminal actions. In most cases, the information security policy is vague – there is a problem with the information system itself (Rogers & Buffalo, 1974; Sykes & Matza, 1957).

Denial of inquiry

In this case, the perpetrators justify their criminal action by saying it will not harm anyone to remove any excuse for a crime (Siponen & Vance, 2010; Sykes & Matza, 1957).

Defence of necessity

In this rationalization technique, insiders justify that there was no other option other than committing the crime. They usually provide a reason such as "I needed to cover medical costs for my son" (Piquero, Tibbetts & Blankenship, 2005).

Condemnation of the condemners

In this technique, the fraudsters will put the blame on others to justify their criminal activities (Byers, Crider & Biggers, 1999); for instance, they may say, "My boss has denied me a promotion and he is the one to be blamed for my criminal act."

Appeal to higher authorities

In this case, the perpetrators assume that their criminal actions are justified, as they think that they are doing it to achieve the organizational objectives (i.e. an urgent job order) in the process violating the security policy of the organization (Piquero et al., 2005).

The Metaphor of the Ledger

In this rationalization technique, offenders may justify that they have contributed significantly to the organization's effectiveness, such as producing an innovative solution to a problem. They then rationalize that they need to be excused for breaching the information security of the organization (Klockars, 1974; Piquero et al., 2005).

3.2.2.4 Capability

Capability refers to the ability to carry out the planned fraudulent activities. According to the fraud triangle, criminals require the ability, skill, and mindset to commit a crime even though they may be motivated. The fraudsters also require the skill to identify any gap in the information system of the organization. Consequently, they plan their attack and need knowledge of how to bypass any security protection that the organization has devised to protect the system, both from internal and external threats. Capability is also related to psychological factors like personal traits, character, learned behaviours and the confidence of the fraudsters to commit a crime.

3.2.3 Application of the Fraud Diamond

The fraud triangle may be used to predict fraud risk factors in addition to detecting a committed fraudulent act (Skousen et al., 2009) so as to predict which employees are likely to be involved in fraudulent activities. Skousen et al. (2009) propose that publicly available fraud cases can be used to determine which organizations are more likely to be involved in crime. They have developed different variables that serve as proxies for pressure, opportunity, and rationalization. They have also tested their model with samples of real-world fraud data, using multiple discriminant and sensitivity analyses, and found these effective for making predictions.

Brown et al. (2013) propose an architecture that differentiates between suspicious and non- suspicious human behaviour so as to predict fraud incentives and the potential for

rationalization by mining user data. They argue that the mood of users can be determined by analysing word choice and frequency in their e-mail communication as well as monitoring their behaviour by using network analysis and process logs.

This study argues that the identification and prediction of fraud risk elements can supplement the effort to mitigate insider threat, using situational crime prevention (SCP) techniques. Identifying those elements that create opportunities for insider threats will be used to reduce the opportunity for crime in SCP.

The detection of employees are under pressure to commit a crime may assist an insider threat detection system to warn the insiders on the risk of any planned criminal acts and their violations of IS security policy of the organization so as to remove any excuse that insiders use for committing a crime. Focusing on rationalization elements of the fraud triangle will help in identifying the justifications that offenders use when committing a crime. These elements may be used in eliminating future justifications such as the absence of clear rules in SCP.

This study has adopted the Fraud Diamond and proposed an insider threat prediction and prevention model. The model is discussed in detail in chapter five.

This research also uses situational crime prevention (SCP) techniques to remove any rationalization from committing a crime. This is only one component of the Fraud Diamond. SCP is discussed in detail in the next section.

3.3 Situational crime prevention (SCP)

3.3.1 Definition of SCP

As defined by Clarke (1997):

> "Situational prevention comprises opportunity-reducing measures that (1) are directed at highly specific forms of crime, (2) involve the management, design or manipulation of the immediate environment in a systematic and permanent way as

possible, (3) make crime more difficult and risky, or less rewarding and excusable as judged by a wide range of offenders" (p.54).

First, the definition emphasizes that SCP focuses on highly specific forms of crime, and a distinction must be made between the different kinds of offenses that are categorized under broad crime categories like burglary and robbery. The second point of the definition is that SCP assumes that everyone has the probability of committing a crime if the opportunity allowed the person to do so. Therefore, SCP techniques assume that there will be different motivations for crimes, and design a technique that will be applicable to all without making any distinction between criminals and others. The third important idea of the definition is that it assumes that offenders will make cost-benefit analyses before committing a crime. SCP works on increasing the risks of committing a crime when compared to the benefits that offenders anticipate to gain from it. The fourth area of focus of SCP is to neutralize any justification that offenders use to commit a crime by increasing the costs of committing a crime and decreasing any excuse for committing a crime. The final emphasis is that SCP should be designed as a general solution without specifically mentioning any type of crime.

3.3.2 Theoretical background of SCP

The idea of situational crime prevention was first initiated by a study conducted by the British Home Office with the intention of reducing factors that facilitate crime, such as places and situations (Clark, 1983). Clark (1995) hypothesized that offenders analyse the risks, benefits, and the efforts needed before becoming involved in the crime. Offenders will decide to commit a crime when they think that the benefits outweigh the risks and the efforts associated with the crime.

There are three basic theories that have been used as a basis for SCP. These theories are rational choice, routine activities, and lifestyle perspectives. The core idea of SCP is that offenders will commit a crime when they have the opportunity, and they make a choice to commit a crime. The rational choice theory claims that offenders make a decision to commit a crime, based on their analysing various factors such as efforts needed, the risk

to be caught, the benefits, availability of collaborators, and the needs of the offenders (Clarke & Cornish, 1985; Cornish & Clarke, 1986). It may not always be true that all offenders have a free will to choose; rather, they mostly decide by assessing those factors before making a decision.

In addition to the factors discussed above, the choice to commit crime, offenders also depend on their daily routines. Routine activities theory states that the daily activities of individuals will affect the convergence of motivated offenders when they have the opportunity to attack a target that is without any guardian to protect it. Cohen and Felson (1979) demonstrated that the availability of homes without guardians during the day, together with the availability of portable valuables resulted in increasing burglary levels in Britain during the 1960s.

Not only the choice and routines that are more related to the offenders but also the lifestyle of the victim affect the occurrence of crime (Garofalo, Gottfredson & Hindelang, 1978). For instance, an individual who frequently does exercise in nighttime outside of his/her household can be more likely to be victims by criminals.

The choice of the offender to commit a crime will be affected by factors such as risk, benefits, and efforts needed as well as the daily routine and lifestyle of individuals. Therefore, the major emphasis of SCP is to discourage offenders from choosing to commit a crime by increasing the risk and the efforts required to commit a crime and reducing the benefits of committing a crime.

3.3.3 Techniques of SCP

Clarke and Eck (2005) propose five major aims of SCP to mitigate a crime. Their aims are: “

- Increasing the effort required to commit a crime by target hardening or by controlling access to targets or the tools required to commit a crime.
- Increasing the risks by increasing the levels of formal or informal surveillance or guardianship.

- Reducing the rewards by identifying the property in order to facilitate recovery by removing targets or by denying the benefits of crime.
- Reducing provocations by controlling peer pressure or by reducing frustration or conflict.
- Removing excuses by setting clear rules and limits." (p 74)

Homel and Clarke (1997) argue that "if offenders can be prevented from rationalizing and excusing their criminal acts, then they will be open to feelings of guilt and shame, which reduce crime" (p.19). Among the five aims of SCP, this research will use removing excuses as a prevention technique.

Cornish and Clarke (2003) propose five techniques for removing excuses, including setting rules (e.g. harassment codes), posting instructions (e.g. "No Parking"), alerting conscience (e.g. roadside display boards), assisting compliance (e.g. easy library checkout) and controlling drugs and alcohol (e.g. alcohol-free events). Willison and Siponen (2009) proposed two remove-excuse techniques that may be used in the information security domain. These techniques are an information security policy (setting rules) and security education for staff members (assisting compliance).

Cornish and Clarke (2003) propose 25 techniques that may be used to reduce the opportunities for a crime under the five aims of SCP. Among these are "target hardening (e.g. anti-robbery screens), controlling the access to facilities (e.g. electronic card access), controlling tools/weapons (e.g. password-protected electronic devices), assisting natural surveillance (e.g. building design with clear visibility), reducing frustration and stress (e.g. fair compensation for employees)" (p. 79).

3.3.4 SCP for computer crime

Recently, interest has been shown among information security researchers to borrow the concept of SCP from the criminal theory and apply it to cybercrimes. Beebe and Rao (2005) argue that current IS security focuses on offenders and not on crime environments

though many of the SCP techniques are implicitly applied in IS security solutions. They have also extended the SCP techniques to external threats in addition to insider threats. Willison and Siponen (2009) have justified that the 25 techniques can be mapped to information security, specifically to address the insider threat problem. Padayachee (2013) and Padayachee (2015b) provides a conceptual framework to mitigate the insider threat from an opportunity-based perspective. Padayachee (2015a) also proposes an insider threat neutralization mitigation model, based on the SCP theory, the neutralization theory, and the cognitive dissonance theory. However the framework and model did not consider the motive and capability component of fraud diamond which are also important factors to mitigate insider threat.

Research that tries to justify the application of SCP to specific cybercrimes such as Me and Spagnoletti (2005) for online pedo-pornography and Reyns (2010) for cyberstalking victimization has been conducted. However, both of the works focus on minimizing the opportunity for crime without considering on addressing the motive and capability elements to commit a crime. Beebe and Rao (2005) have made a digital analogy for 16 opportunity-reducing techniques, as proposed by Clark (1997). The analogy is presented in Table 3.1.

Table 3.1 Sixteen Opportunity-Reducing Techniques (adopted from Beebe and Rao, 2005)

	Opportunity-Reducing Technique	**Physical Crime Analogy**	**Digital Crime Analogy**
Increase Perceived Effort	1. Target Hardening	Locks, safes, fences, barriers,	Firewalls, closed ports, vulnerability patches
	2. Access control	Gate codes, guard shack, receptionist, swipe cards	ID/authentication systems, digital certificates
	3. Deflecting offenders	Pedestrian / auto-traffic redirection, no loitering	Honeypots/honeynets, information segregation
	4. Controlling facilitators	Gun control, limit ability to communicate	Masking IP addresses, leased lines, no broadcast
Increased Perceived Risk	5. Entry/exit screening	Metal detectors, screeners, merchandise	Intrusion detection system, virus scanning
	6. Formal surveillance	CCTV, security guards, police	Auditing and log reviews, anomaly detection
	7. Surveillance by employees	Responsibility and/or ability to monitor	Resource usage of info, user training, reporting policies
	8. Natural surveillance	Lights, etc. so passers-by can see activity in the building	Tamper-proof network cabling, visualization tools

Decrease Anticipated Reward	9. Target removal	Electronic donation vs. cash, cash diverted to safe	Information and hardware segregation, DMZs
	10. Identifying property	VIN etched in audio glass, write name in the book	Information classification, watermarking
	11. Reducing temptation	Obscure valuables, gender-neutral phone book	Minimize reconnaissance info, no port bannering
	12. Denying benefits	Security coded car radios, ink tags on clothing	Encryption, automatic data destruction mechanisms
Remove Excuses	13. Rule setting/ clarification	Acceptable use policy, clear laws, licensing	Acceptable use of policy, user agreements, clear laws
	14. Stimulating conscience	"Shoplifting is stealing" signs, Current speed	Multi-level warning banners, code of ethics
	15. Controlling disinhibitors	Controlling drugs/ alcohol, propaganda,	Cyber-ethics education, supervised computer use
	16.Facilitating compliance	Graffiti boards, public urinals, shelters, barriers	Hacker challenges, employment opportunities

This study has adopted the techniques for removing excuses of the situational crime prevention techniques to remove excuses for an insider threat and to assist with compliance as part of the proposed insider threat prediction and prevention model. The techniques have been deployed as guidelines for change management in future mitigation of insider threats. The model is discussed in detail in chapter five.

For both the Fraud Diamond and SCP, there is a need to collect information about insiders such as their motives, capabilities, rationalizations, and responses to current criminal opportunity. The model proposes to use context-aware systems to collect current information. These systems will be discussed in detail in the next section.

3.4 Context-aware systems

One of the limitations of the current insider threat detection and prevention model is that it depends on previously collected sources of data, which are not reliable. For instance, the model proposed by Kandias et al. (2010), is based on information collected from human resources data. However, this data may not reflect the current behaviour of insiders. While some models collect data from employees but this information is not reliable, as insiders may provide false information (Memory, Goldberg & Senator, 2013). Therefore, there is a need to automatically collect up-to-date information about insiders that may be collected using context-aware systems.

3.4.1 Context

According to Dey (2001), "context can be defined as any information that can be used to characterize the situation of an entity" (p.6). "An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including location, time, activities and the preferences of each entity" (Dey, 2001, p.6). Brown, Bovey and Chen (1997) define the term 'context' as a function of the location of an entity, identities of users around the entity and changes with the variables of the objects (e.g., season and temperature). Ryan, Pascoe and Morse (1999) refer to the term 'context' as the location of users, their environment, their identity and the time at which the event has happened.

According to Klompmaker, Nebe, Busch and Willemsen (2009), context parameters may be classified into two categories, namely the outer context and the inner context. The

outer context refers to anything that surrounds the user such as the location, the environment or the operated hardware, whereas those contexts within the inner world of the user such as experiences, goals, needs, motivations, feelings, cognitive structures and processes are categorized under the inner context.

3.4.2 Context-aware interface

Context-aware interfaces provides a user with a very effective and user-friendly interface, depending on the situation in which the user is in currently, the collection of people nearby, hosts and accessible devices as well as changes happening over time (Schilit, Adams & Want, 1994). Such applications are very important, especially in today's environment where mobile devices such as smartphones are widely used. The user context can be gathered from different sensors, including GPS receivers, accelerometers, gyroscopes, digital compasses, and proximity and ambient light sensors. Context is very important since it provides information about the present status of people, places, objects such as devices in the environment (Korpipaa, Mantyjarvi, Kela, Keranen & Malm, 2003; Kwon, 2004).

Context-aware applications are expected to adapt to specific contexts so that they can meet users' preferences. Dobre, Manea and Cristea (2011) have attempted to categorize context applications into those that adapt at runtime in the present context and those that store the contexts and adapt at a later stage (namely passive applications).

There are various initiatives to apply context-aware interfaces in different domains. For instance, Ancona, Bronzini, Conte and Quercini (2012) propose a context-aware interface called the Agamemnon system, which guides tourists by providing information only relevant to current monuments that they are visiting.

Muñoz, Rodríguez, Favela, Martinez and González (2003) propose a context-aware application for medical doctors, which checks the ward where the doctor is currently working and provides him with a list of drugs only related to the ward during prescription so that it will save screen usage and the physician's time. Further research has been

conducted on the applications of the context-aware system. They include context-aware user interfaces for online exercise training supervision (Klompmaker et al., 2009) and context-aware browsers incorporating intelligence systems (Coppola, Della Mea, Di Gaspero, Menegon, Mischis, Mizzaro, Scagnetti & Vassena, 2010).

3.4.3 Application of context-aware systems to the information security domain

Various research studies have attempted to apply context-aware systems specifically to the information security domain. Al-Muhtadi, Ranganathan, Campbell and Mickunas (2003) have presented a ubiquitous security mechanism that integrates context-awareness with automated reasoning to perform authentication and access control in ubiquitous computing environments. Wullems, Looi and Clark (2004) also propose context-aware authorization architecture to augment existing network security protocols in an intranet environment. Lee, Yang, Jun and Chung (2007) applied "context-aware systems to security services, providing multiple authentications and authorizations from a security level, which is decided dynamically in a context-aware environment" (p.303). An, Bae, Kim and Seo (2009) propose a context-aware dynamic security configuration scheme for effective security management of the mobile communication device. Hu and Weaver (2004) also propose the application of context-aware security infrastructure for healthcare industry applications. They propose a model that is capable of making authorization-based contextual information like time, location and the authentication trust level of users available.

Georgiadis, Mavridis, Pangalos and Thomas (2001) and Wang (1999) propose a team-based access control which is aware of the contextual information. Georgiadis et al. (2001) propose a model that assigns permission in a team-based approach with the argument that a collection of the user who is working in a specific task accessing a common resource by the user should be context aware. In their model, 'context' refers to the ongoing activity of the team and users who are involved in the activity so that

permission will be granted to users, specifically for the activity in which they are currently engaged.

Wang (1999) argues that access control should be managed, based on the current activity of the team but he proposes that permission should be granted to roles rather than individual users. Watanabe, Yamada, and Nagatou (2003) propose a security architecture that is based on context-aware systems to enforce security policies at run-time by using process algebraic language constructs. In their architecture, 'context' refers to external events like the location of a device and internet connection as well as history-sensitive behaviours. They enforce the security policies based on these contexts.

Brown et al. (2013) propose an architecture that includes the prediction of fraudulent behaviours by studying the mood of users by text-mining the word choice and frequency in their electronic communication. They argue that individuals who are at risk for insider threats may be predicted, based on analyses of contexts related to their electronic communication, including e-mail messages, social media posts and chat sessions which reveal much about their psychological status. They propose that the result of the prediction can be used for proactive mitigation through coaching and assistance programs as well as termination of employment, as it is required (Brown et al., 2013).

Shaw and Fischer (2005) argue that 80% of the insider threat risks can be prevented by avoiding psychological problems like anger, anxiety, stress and psychological impairment of employees.

In this study, a context-aware system is applied to gather information about offenders' inner contexts, including their motives to commit a crime and considering factors like their stress levels and emotions as well as their resource usage behaviour. The use of contextual information is useful in information security as it gathers current information about insiders which might not be available in human resource data. Using current contextual information will be useful to take immediate action when there are any information security violations without delay. The details are discussed in chapter five.

3.5 Privacy-preserving techniques

Most of the current insider threat prediction and prevention models do not consider the privacy issue when conducting workplace monitoring. Monitoring the employees may affect them negatively and cause stress, low commitment, and lower productivity (Brown, 1996; Dhillon & Moores, 2001). Their private information may be made available to intruders during transfer of data (Greitzer & Frincke, 2010) so there is a need to balance privacy issues when designing and implementing insider threat mitigation strategies.

According to Saranya et al. (2015), privacy-preserving techniques can be categorized into three categories, namely the randomization method, anonymization and distributed privacy preservation. Each of these techniques will be discussed next.

3.5.1 The randomization method

The randomization method adds data distortion to create a private representation of the records to allow mostly the recovery of aggregate distributions rather than the recovery of individual records (Saranya et al., 2015). The model of randomization is presented in Figure 3.4.

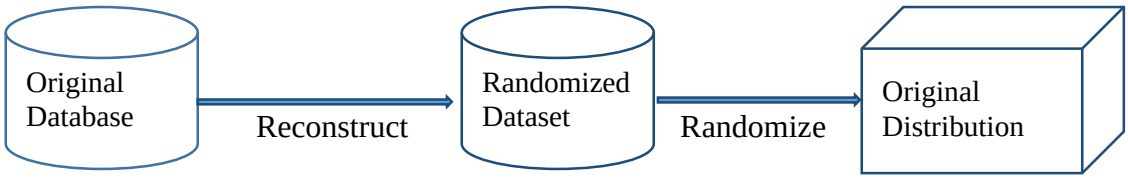

Figure 3.4 Model of Randomization (Saranya et al., 2015)

In the randomization method, there are two types of perturbation: addictive perturbation and multiplicative perturbation. The former adds randomized noise to the database and the overall data distribution will be recovered later, whereas the latter uses random projection or random rotation techniques for perturbing the records.

The advantage of randomization is that it greatly helps to preserve individual sensitive data. It is also very easy to implement, as it can be applied in the data collection phase and there is no need to collect other knowledge – thus there is no need to secure a server for the system.

3.5.2 The anonymization method

The anonymization method focuses on removing explicit identifiers so that the identity of individuals in the sensitive database will be protected. Therefore, this method addresses the risk with identity and attribute disclosure (Saranya et al., 2015). Identity disclosure refers to when an individual is uniquely identified from the released data whereas attribute disclosure refers to scenarios where the identity of individuals is inferred from other attributes from the released sensitive data. There are three popular techniques of anonymization; these are k-anonymity, l-diversity, and t-closeness.

The following two tables illustrate the process of anonymization. Table 3.2 shows the original data and Table 3.3 shows the data after it has been anonymized. The zip code and the ages have been changed to another format to avoid any use of the zip code identifying any individuals.

Table 3.2 Original patterns table (adapted from Gkoulalas-Divanis and Loukides, 2013)

S.NO	Zip Code	Age	Disease
1	546177	39	Heart Disease
2	546102	32	Heart Disease
3	546178	37	Heart Disease
4	549105	53	Gastritis
5	549209	62	Heart Disease
6	549206	57	Cancer
7	546205	40	Heart Disease
8	546273	46	Cancer
9	546207	42	Cancer

Table 3.3 A3 - Anonymous version of Table 3.2 (adapted from Gkoulalas-Divanis and Loukides, 2013)

S.NO	Zip Code	Age	Disease
1	546***	3*	Heart Disease
2	546***	3*	Heart Disease
3	546***	3*	Heart Disease
4	549***	>=50	Gastritis
5	549***	>=50	Heart Disease
6	549***	>=50	Cancer
7	546***	4*	Heart Disease
8	546***	4*	Cancer
9	546***	4*	Cancer

The anonymization technique presented table 3.3 is useful for insider threat detecting systems as key identifiers in insider data will be replaced by other characters which makes it impossible to identify the insiders, which in turn preserve the privacy of insiders.

3.5.3 Distributed privacy preservation

Distributed privacy preservation techniques apply when there is a need to carry out a joint computation from different datasets so that the privacy in individual datasets will be preserved (Saranya et al., 2015). There are two settings to implement this method. The first runs a union of algorithms in different databases and disallows any one of the databases to view the individual data in each database. The second setting modifies the individual datasets so that sensitive data will be protected, and at the same time, it runs a joint operation on modified datasets.

In this study, the anonymization technique is selected to preserve the privacy of insiders as it removes any identifiers that may help in identifying insiders from the information collected by the model proposed in this research. All identifiers that might be used to uniquely identify an insider have been anonymized by replacing the identifiers with another character which is completely secure. The details are discussed in section 5.3.3.

3.6 Chapter summary

This chapter has reviewed different theories from criminology, psychology, and computer science that are adopted to the model presented in this research. The model is based on the Fraud Diamond, which is borrowed from the discipline of criminology and discussed in detail in this chapter, including its application to the information security domain (see section 3.2). This research has also adopted situational crime prevention techniques and neutralization mitigation from the discipline of criminology (see section 3.3). These constructs are used to remove any excuse for a crime. The relevant theories are discussed in detail in this chapter. In addition, a context-aware system from the discipline of computer science has been added to the model to collect contextual information related to motive and capability of insiders, both of which are reviewed in this chapter (see section 3.4). Finally, techniques for privacy preservation are discussed and one of the techniques (anonymization) has been adopted in the model proposed in this research to preserve the privacy of insiders (see section 3.5). The concepts are presented together in Table 3.4.

Table 3.4 Summary of concepts

Concept		**Purpose**
Fraud Diamond	Pressure	Insider prediction
	Opportunity	Insider prediction
	Capability	Insider prediction
	Rationalization	Insider threat prevention
Neutralization techniques		Insider threat prevention
Situational crime prevention		Insider threat prevention
Context-aware system		Insider prediction and privacy preservation
Anonymization		Privacy preservation

The next chapter will discuss in detail the research methodology that is used in this study to address the insider threat problem.

CHAPTER FOUR

Methodology

4.1 Introduction

This chapter discusses the research paradigm that is applied to this research, which is design science research. The chapter also discusses in detail a research methodology that is adopted for the research that is called the Design Science Research Methodology for Information Systems Research by Peffers et al. (2007). Each process of the research methodology is discussed in comparison to how it has applied and developed the artefact in this research, namely a **P**rivacy-Preserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction model (PPCAITPP). The whole research process is mapped to the chosen methodology and will be discussed in this chapter. Finally, the chapter discusses the validation of the research methodology, based on seven design science research guidelines proposed by Hevner et al. (2004). The research methodology validation will also be discussed in comparison to the research process followed to develop the model proposed in this research.

4.2 Research paradigm

Information systems is a multidisciplinary field which borrows theory from different fields such as computer science, social sciences, law, business and so on (Bariff & Ginzberg, 1982; Avison & Myers, 1995; Baskerville & Myers, 2002). Because of its multidisciplinary nature, there is confusion over what research paradigm and research methodology are to be used for IS research (Benbasat & Zmud, 2003; Klein, 2003; Mingers, 2001; Nunamaker, Chen & Purdin, 1990).

There are two types of scientific research in information systems, namely descriptive and prescriptive research. Descriptive research is more related to the natural sciences that

attempts to understand the nature of information technology itself, like explaining how and why things are the way they are (Hempel, 1966). Prescriptive research is related to design sciences like the engineering disciplines which is applicable to this research. These disciplines produce artificial knowledge (artefacts) to attain goals like improving the performance of IT (Simon, 1996).

The popularity of design science information systems is increased in the information systems discipline as a result of its very important contribution to addressing two basic issues in the discipline. The first issue is the increasing role of IT artefacts in IS research (Benbasat & Zmud, 2003; Orlikowski & Iacono, 2001; Weber, 1987) and the second issue addresses the criticism of the discipline that it lacks research that produces new knowledge (Benbasat & Zmud, 1999; Klein, 2003).

The design science research paradigm is gaining more popularity in information systems research and its importance to the discipline is underlined by various authors such as Gregor (2002), Gregor and Jones (2007), Hevner et al. (2004), Iivari (2007), Kuechler and Vaishnavi (2008), Peffers et al. (2007) and Vaishnavi and Kuechler (2004). According to a definition suggested by Iivari and Venable (2009), design science research can be defined as a research activity that invents or builds new, innovative artefacts for solving problems or achieving improvements. They claim that design science research (DSR) creates new means for achieving some general (unsituated) goal as its major research contribution. Such new and innovative artefacts create a new reality, rather than explaining the existing reality or helping to make sense of it (Iivari & Venable, 2009).

The purpose of DSR in information systems is to develop and evaluate IT artefacts with the aim of solving organizational problems (Hevner et al., 2004). This purpose goes hand-in-hand with the goal of this research, namely to solve insider problems by developing an artefact or a model by integrating different theories from the fields of computer science, criminology, and psychology. Thus, the researcher has selected design science research as research paradigm for this study.

4.3 Research methodology

For this research, the research methodology called Design Science Research Methodology for Information Systems (IS) Research by Peffers et al. (2007) has been adopted and follows the whole process of their methodology which is based on three objectives, namely:

I. It should be consistent with existing related methodologies that are available in literature in the IS discipline and other related disciplines.

II. It should be used as a nominal process model for IS researchers who employ design science research as their research paradigm.

III. It should provide IS researchers with a mental model that will be used to present and evaluate IS research conducted based on design science research.

Peffers et al. (2008) proposed a process model for DSR for information systems research after extensively reviewing and synthesizing ideas from seven well-established papers on design research from IS and other disciplines, as presented by Archer (1964), Eekels and Roozenburg (1991), Hevner et al. (2004), Nunamaker et al., (1990); Rossi and Sein (2003), Cole, Purao, Rossi and Sein (2005), Takeda, Veerkamp and Yoshikawa (1990) and Walls, Widmeyer and El-Sawy (1992).

The process model proposed by Peffers et al. (2008) consists of six elements:

I. Problem identification and motivation

II. Objective of a solution

III. Design and development

IV. Demonstration

V. Evaluation

VI. Communication

Each element of the process model will be discussed relating how it is applied in this research as a **P**rivacy-Preserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction model.

As is shown in Figure 4.1, the first step involves developing a new model by reviewing existing models related to insider threats. The purpose of the second step to prototype the model into an executable version. The third step is for validation where expert opinion on the proposed model is collected from a panel of experts from the insider threat domain. The evaluation is done in two iterations. Finally, the findings of the study will be communicated to the academics and professionals, using conference presentations and a publication in a journal.

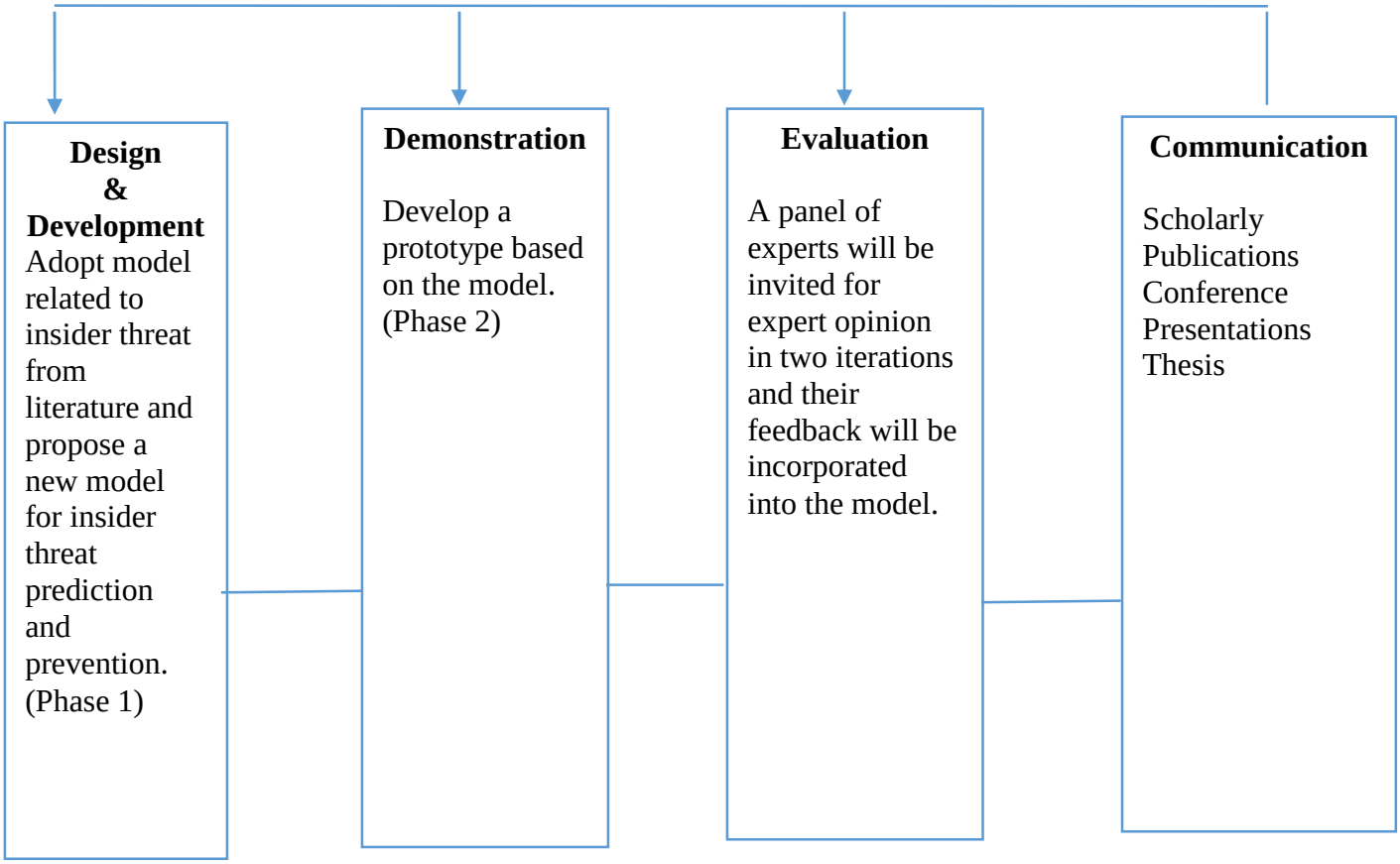

Figure 4.1 Research model (adapted from Peffers et al., 2007)

4.3.1 Problem identification and motivation

The magnitude of the insider threat problem is huge and as per a study conducted by the SANS Institute (2015), 74% of information security professionals who participated in the study reported that insider threats are a serious concern for their organizations. From the participants who participated in the same study, 32% of them reported that they did not have any security system to mitigate insider threats and this makes them very vulnerable. According to a survey conducted by the International Business Machines Corporation (IBM), 55% of the cybercrimes are committed by insiders (IBM, 2015). This shows the insider threat is a serious concern to be addressed. Tackling insider threats is challenging, as insiders are trusted by the organization and provide a credential to access information resources of the organization. The issue is complicated because insiders are diverse and their behaviour changes dynamically which makes it extremely challenging for mitigating insider threats (Sharghi & Sartipi, 2016).

Another challenge with mitigating insider threats is privacy issues, as insiders expect their privacy to be protected during implementing any monitoring of their activities such as their communication in social media and e-mails to identify insiders. Consequently, the insider threat problem requires an integrated solution, which takes into consideration the diverse and dynamic nature of insiders with preserving their privacy. Organizations need such solutions to implement any security system to address insider threats.

4.3.2 Objectives of a solution

The major objective that drove this research is to propose a new insider threat prediction and prevention model that is derived from extant models to address the insider threat problem. The model leverages experts in the IS security area. The model considers all contexts related to insiders including psychological, cultural, organizational and social factors.

A second objective of the model was to study and adopt solutions, which had been developed to address insider threats outside of digital security, as there common factors shared in physical and cyber security.

Finally, the research aimed to propose a comprehensive model that would preserve the privacy of insiders as much as possible because employees require privacy in their workplace. Consequently, they might become frustrated and their productivity might decrease. The employees' data might also be exposed to intruders during data transfer and back-ups unless the data is anonymized to remove identifiers.

4.3.3 Design and development

To achieve the objectives of the solution, a critical review of extant literature was conducted to address the insider threat problem. Based on the literature review, the Fraud Diamond is used effectively to solve threats posed by insiders. In the IS domain, insiders require motive, opportunity, capability, and rationalization to commit a crime, just as other crimes. Context-aware systems are proposed to collect current information about insiders related to motive and ability as well as to determine whether insiders exploit any opportunity to commit a crime. The model is required to work in real-time because insiders can be tempted to become involved in malicious activities. For the purposes of determining whether a high risk insider can be baited into maliciousness, honeypot is facilitated to lure them into committing a crime.

One of the factors for committing a crime is rationalizing the criminal act in order to nullify any justification for their crime by implementing neutralization mitigation techniques. The removing excuse techniques of situational crime prevention such as post-instruction (i.e. e-mail disclaimers), alert conscience (i.e. a code of ethics), and assist compliance (hacker challenges) to remove any excuse to commit a crime are deployed. In addition, it is proposed that a technique of setting rules (i.e. policy) that explicitly invalidate any potential defences (i.e. excuses) for cybercrime may be a useful mitigation strategy. This implies resetting the rules, based on new justifications for cybercrime.

The concept of a context-aware system was used to leverage the following dimensions and interactions:

1) *Motivation*: by monitoring the interactions of insiders with the system (i.e. considering metadata such as search behaviour, file access, logins, keystrokes)

2) *Capability*: by monitoring insiders' usage of computer applications as well as system warnings and errors

3) *Opportunity*: by monitoring the insiders' interaction with the honeytoken that is deployed to lure suspicious insiders

4) *Rationalization*: monitoring the suspicious insiders' interaction with the neutralization mitigation to identify and nullify their justifications to prevent future crime

The model preserves the privacy of the insiders, as all of the information is anonymized to remove identifiers that may help to identify a specific insider. This is accomplished in the following ways with respect to each dimension:

1) *Motivation*: The motivation is not identified; rather, the metadata associated with an insider who is motivated to commit a cybercrime is collected.

2) *Capability*: Their capability is assessed in terms of only their application usage and they will not be uniquely identified.

3) *Opportunity*: The honeytokens are deployed anonymously to lure suspicious insiders.

4) *Rationalization*: The information from the neutralization mitigation is collected anonymously.

4.3.4 Demonstration

To demonstrate the feasibility of the artefact, the model implemented a concept/prototype by using an asset management system as a case study. Java is used for programming and MySQL is used for the database management. The prototype assessed the context of

insiders related to their motive and capability by using their resource usages behaviour, such as their typing patterns and the number of warnings and errors like pressing the wrong character with the frequency of errors.

The result of the analysis of the contexts will be presented to management to identify high-risk insiders anonymously, and these results will authorize the facilitation of a honeypot to high-risk insiders. Following the prototype will add one additional link as a honeytoken and an opportunity to lure insiders to commit a crime. If the insiders click on the honeypot, they will be warned that accessing the link falls outside of their authorization level. They will then be asked if they still wished to continue accessing the particular information. If they continue insisting on accessing the honeytoken, they will then be asked to provide their rationalization for accessing the unauthorized link. Finally, based on their justification, their excuses will be nullified, based on neutralization mitigation techniques and the remove-excuses techniques of SCP. This notion is done in order prevent future crime.

4.3.5 Evaluation

This research has adopted four basic principles to which IS research should conform, as proposed by Österle et al. (2011). The principles have been adopted because they are supported by more than 110 full professors of information systems and related areas to be used as a standard for any information systems research, using the design science research methodology. The principles are briefly discussed below.

1) *Abstraction*: The artefact must solve a class of problems in some domain.

2) *Originality*: The artefact must contribute substantially to the advancement of knowledge in the IS discipline.

3) *Justification*: The artefact must be justified in a comprehensive manner and validated with its feasibility.

4) *Benefit*: The artefact must benefit its stakeholders, either immediately upon design or in the future.

In addition, the model was evaluated in terms of its viability (i.e. feasibility of the model), utility (i.e. value), efficacy (i.e. effectiveness), usability and scalability. Based on these principles, the researcher designed a questionnaire to be completed by twenty-six panel experts who were selected from the industry and the academia. The research employed both qualitative and quantitative data collection methods. A questionnaire was adopted from Padayachee (2015a), containing both open-ended and structured questions (see Appendix A). The structured questionnaire was used to collect feedback from the expert panel members related to the model concepts of viability (i.e. feasibility of the model), utility (i.e. value), efficacy (i.e. effectiveness), usability and scalability.

The in-depth interview method was used for participants to provide their feedback on the research rigor, based on the four principles proposed by Österle et al. (2011). These researchers proposed to evaluate design science research in information systems.

As a reference for the experts, the description of the model concept, a presentation video of the model as well as proof of the concepts were made available online at https://sites.google.com/site/citppmodel/. The experts evaluated the model after analyzing both the model and the proof of concepts, where after they provided feedback by completing a survey in two iterations. The prototype was presented by means of video demonstrations rather than using a hands-on in order to expedite the process. Since the participants' evaluation was done mainly on the proposed model and the prototype was used to demonstrate the model, the video demonstrations did not limit the evaluation. Their feedback was reviewed by the researcher and used to refine and improve the model. Based on the feedback, the model, proof of concepts, prototype and the questionnaire which were presented for evaluation of the second iteration were revised.

4.3.6 Communication

The results of this research were communicated to the scientific community by means of a presentation in an international conference and published in the proceedings of the

conference in IEEE. The reviwers accepted the model presented in the paper as innovative in the application of a honeypot, situational crime prevention, and fraud diamond and context aware system into the organizational structure of insider threat mitigation. They also gave positive feedback in the privacy-preserving feature of the model.

4.4 Research methodology validation

The research methodology adopted for this research was evaluated, based on seven design science research guidelines proposed by Hevner et al. (2004). Each guideline and its application in this research is discussed next.

4.4.1 Guideline 1: Design an artefact

The major output of IS design science research is an innovative artefact that can be used by practitioners and the industry to develop an information system, based on the proposed artefact. A novel privacy-preserving, insider threat and prediction model which is an artefact that can be used for organizations and individuals to develop an insider threat prediction and prevention system as well as security procedures and policies are proposed.

4.4.2 Guideline 2: Problem relevance

The artefact proposed in this research addresses a serious insider threat problem, which is challenging to tackle, as insiders have access credentials and they know in detail the internal working of the organization. Another challenge with the problem is that insiders are people, and it is complicated to understand and predict their behaviour. The reason is that each person has his or her own behavioural patterns and traits and these factors make it challenging to address. This artefact solves the problem of privacy abuse by monitoring

the activities of insiders, such as their electronic communication, for detection and mitigation. The model attempts to preserve the privacy of insiders. The complexity of the problem requires the use of different theories from the disciplines of criminology and computer science.

4.4.3 Guideline 3: Design Evaluation

One of the evaluations proposed by Österle et al. (2011) is involving experts in the domain area of the problem to evaluate the artefact. For this research, a panel of 26 IS security experts (n=26) was gathered from the industry and academia to evaluate the model as well as the prototype. They evaluated the model based on Österle et al.'s (2011) principles, namely abstraction, originality, justification and benefit. The evaluation was done in two iterations with the revision of both the model and the prototypes as per the suggestions by the panel of experts until they were satisfied with the feasibility of the model. The details of the contribution are discussed in chapter eight.

4.4.4 Guideline 4: Research contribution

According to Henver et al. (2004), there may be two research contributions at the end of DSR research. The first contribution is the artefact produced and the second contribution is that an improvement should be made to the existing DSR paradigm or methodology. For this research, the contribution is the produced artefact, namely a **P**rivacy-Preserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction model (PPCAITPP). The details of the contribution are discussed in chapter eight.

4.4.5 Guideline 5: Research rigor

This research was conducted, based on rigorous methods to construct and evaluate the artefact. The construction of the artefact was based on the study of extant literature in this field of IS security. The evaluation was conducted by expert opinions proposed in the

literature while the principles of evaluation used in this study were based on acceptable standards in design science research.

4.4.6 Guideline 6: Design as a search process

The model was produced after an extensive review of literature related to insider threats, the Fraud Diamond, situational crime prevention, context-aware systems and privacy-preserving techniques. These components are discussed in detail in the literature review. The model was further improved by experts' opinions in the IS security field with two iterations to refine the model. The model was implemented by creating a prototype to demonstrate the applicability of the artefact and to guide experts in reviewing the model.

4.4.7 Guideline 7: Communication of research

The model was presented to the academics and practitioners in the information security discipline at an international conference. The research was also published for the conference proceedings. The main platform for communicating the results of this research is the thesis itself, as the research is conducted for the fulfillment of the requirements for a Ph.D. degree.

The DSR summary with reference to the chapters in this thesis is presented in Table 4.1.

Table 4.1 DSR summary based on Hevner et al. (2004) with reference to the chapters in this thesis

Guideline	Description	Mapping
Guideline 1: Design as an artefact	The research needs to develop a novel artefact such as a construct, model, method or an instantiation.	Privacy-preserving, context-aware insider threat prediction and prevention model (PPCAITPPM) (Chapter five)
Guideline 2: Problem relevance	The artefact produced must address significant and relevant real-world problems.	Addresses the insider threat problem (Chapter two and chapter five)
Guideline 3: Design evaluation	The artefact developed must be demonstrated and evaluated in terms of research utility, quality, and efficacy.	Prototype, simulation, and expert review (Chapter six and chapter seven)
Guideline 4: Research contributions	The research needs to contribute to the body of scientific knowledge and/or to the design science methodology.	The research combines approaches from criminology and computer science and helps to predict and prevent insider threats while balancing the privacy of insiders (Chapter eight)
Guideline 5: Research rigor	The research must be based on the application of rigorous methods in both	A research methodology, based on extant literature, was used. (Chapter three

	the construction of the artefact as well as the evaluation of the artefact.	and chapter four)
Guideline 6: Design as a search process	The search process to produce an artefact needs to be based on the scientific research process and applied to the context of the specific research problem.	Extant literature was examined in the areas of insider threats, the Fraud Diamond, situational crime prevention, context-aware systems and privacy-preserving techniques based on the principles of design science research. (Chapter two and chapter three)
Guideline 7: Communication of research	The research must be presented effectively, both to technology-oriented and management-oriented audiences.	Thesis write-up and publication (All chapters and Section 4.3.6)

4.5 Sampling

Since the study planned to collect feedback from experts in the IS security field, the researcher used purposive sampling to select the panel of experts. The sample involved information security experts specializing in the insider threat problem and who were employed in a variety of industries. The sample size was 26 (n=26) and approximately 250 security professionals were invited to participate in the study. The response rate was 10%. The feedback from the experts was collected via the internet, using social media platforms like LinkedIn and Google platforms. Participants viewed a demonstration of

the model on YouTube which is available at https://sites.google.com/site/citppmodel. Finally, the study incorporated the relevant feedback into the model in two iterations and the refined model was sent back to the panel for verification.

4.6 Validity and reliability

Design science research procedures require the validation of artefacts produced against the objectives specified, applying the principles proposed by Österle et al. (2011) which are abstraction, originality, justification, and benefit. This study tested the validity of the experts' opinions, based on the level of consensus among them as well as the conformity with existing literature. In order to ensure validity, experts were selected from a variety of industries. Within each domain, the knowledge and skills of the experts were heterogeneous. As the insider threat is pervasive, the skills and knowledge of the experts had to be diversified in order to derive a comprehensive framework. The model framework intended to consider the technological, psychological, socio-technical and organizational dimensions of information systems security. The researcher preserved the anonymity of the participants; hence, the participants did not interact with one another, thus further ensuring the validity of the results. To ensure triangulation of data, the data collection was carried out in two iterations.

According to Nawrockin, Jasiński, Olek and Lange (2005), a scientific experiment should be replicable. The materials, design, procedure, and scoring are described in detail to ease replication. Also, qualitative details are included to account for other factors that may have influenced the study. In order to achieve repeatable results, the study is tested with experts from a wide variety of industries which helped the researcher to evaluate the application of the model in different industries.

4.7 Data collection methods

The research employed qualitative and quantitative data collection methods. A questionnaire was adopted from Padayachee (2015), containing both open-ended and structured questions (see Appendix A.). The structured questionnaire was used to collect feedback from the expert panel members related to the model concepts of viability (i.e. feasibility of the model), utility (i.e. value), efficacy (i.e. effectiveness), and usability (i.e. the degree of ease in using the model) and scalability (i.e. potential to be enlarged).

The in-depth interviews were used by participants to provide their feedback on the research rigor, based on the four principles proposed by Österle et al. (2011) to evaluate a design science research study in information systems. The questionnaire was designed using Google forms and completed online. The confidentiality of the participants' responses was protected. Two versions of the questionnaire were used to collect data. The first questionnaire was designed to collect data in the first iteration and once feedback was received, the questionnaire was revised based on the experts' opinions and redistributed to the experts as a second version.

4.8 Data analysis

Qualitative comments of the participants were categorized manually and listed in the form of frequency counts as well as bar and pie charts for both the first and the second iteration. The researcher prepared two types of questions to collect feedback from the experts, namely structured and in-depth questions. The structured questions were prepared with the intention of collecting the experts' opinions in terms of the practical relevance of the model to insider threats. The structured questions entailed 26 value statements to which participants had to agree or disagree. The participants also had to substantiate their standpoints. A total of five in-depth questions were prepared to validate the research rigor, based on accepted principles of design science. As research rigor principles for evaluation, the researcher adopted the four principles suggested by Österle

et al. (2011) with which IS design science research must comply which are abstraction, originality, justification and benefit.

4.9 Research ethics

To address the ethical consideration for this research, the researcher applied for ethical clearance to the Research and Ethics Committee of the College of Science and Technology (CSET) at the University of South Africa (UNISA) and ethical clearance was granted (see Appendix F).

Participants in the research were provided with an online consent form to sign before they agreed to participate in the study. The consent form is available online at https://sites.google.com/site/citppmodel/test. In the consent form, the purpose of the study was clearly explained together with the research questions to be answered. Participants were informed that the participation in the research was voluntary and they could withdraw from the study at any time. Participants were also guaranteed that the results of this participation were to be kept confidential and would not be released in any individually identifiable form without their prior consent. Possible risks and discomforts participants might face were explained in the consent form.

4.10 Chapter summary

In this chapter, the justification for a research paradigm and a methodology that were applied in this research was provided. The choice of the research paradigm, namely design science research, was discussed in detail (see section 4.2). This chapter also discussed the selected methodology based on information systems research principles proposed by Peffers et al. (2007) (see section 4.3). The discussion of the methodology was carried out with mapping each process followed in the research to confirm that this research had followed a research process based on an acceptable methodology from

extant literature. Finally, the chapter discussed the application of the chosen research methodology in reference to how it was implemented in this research to develop a novel insider threat prediction and prevention model, validating it based on the seven design science research guidelines proposed by Hevner et al. (2004) (see section 4.4).

The next chapter will discuss the artefact produced, namely the **P**rivacy-Preserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction model (PPCAITPP) and how the model was derived from the disciplines of criminology and computer science.

CHAPTER FIVE

A PRIVACY-PRESERVING, CONTEXT-AWARE, INSIDER THREAT PREVENTION AND PREDICTION MODEL (PPCAITPP)

5.1 Introduction

This chapter presents the artefact, namely a privacy-preserving, context-aware, insider threat prevention and prediction model, based on the Fraud Diamond, which comprises four components: pressure (i.e. motive), opportunity, ability and rationalization. First, the chapter discusses the derivation of the model in terms of preventing and predicting insider threats. The chapter also discusses the model and its major components in detail. The model was built on prior research. Finally, the model will be compared with related existing approaches that are proposed to mitigate insider threats by discussing their similarities and differences with the model.

5.2 Derivation of the model

Electronic monitoring is one of the most common approaches to address the insider threat problem, as it can be used to predict any insider threat risk and is able to mitigate after detecting the threat (Yang et al, 2015). Electronic workplace monitoring includes both offline and online activities, including e-mail and social media activities. However, electronic monitoring brings its own challenges, as it invades the privacy of insiders. This may result in loss of mutual trust between employees and the organization, which, in turn, may affect the productivity of the employees negatively (Eivazi, 2011). This negativity can further exacerbate the insider threat problem. Consequently, due to issues of privacy, it is advisable for insider threat solutions to consider preserving the privacy of insiders as much as possible. This research proposes a model which balances the privacy

of insiders. All elements of the model are considered with respect to preserving their privacy.

The model is predicated on the Fraud Diamond which argues that there are four elements that have to be present in order for a crime to occur, namely motive, opportunity, capability and rationalization. The elements of the Fraud Diamond are assessed, based on current contextual information about insiders without collecting any content information to balance privacy issues. For example, the contents of e-mails and social media posts are excluded to protect the privacy of insiders, as this type of data may contain personal information about them. Moreover, once the insider is detected as being suspicious, based on elements of the Fraud Diamond, the prevention is focused on educating insiders so that they will not commit a crime without process occurs without releasing the identity of the insider.

The model is based on two basic elements, namely prediction and prevention which will be discussed next. Insiders are detected as "suspicious" under certain parameters based on motive, capability and opportunity. The prediction is based on the detection probability that the insider is a risk to the organization's information assets. The prevention component is achieved by firstly detecting the probability that the insider is a risk and then using neutralization mitigation to nullify their justifications.

5.2.1 Detection probability

Elements of the Fraud Diamond have been used by various authors to predict future insider threats (Brown et al., 2013; Kandias et al., 2010; Hoyer, Zakhariya, Sandner, & Breitner, 2012). The fraud triangle has been used by Brown et al. (2013) to predict future insider threats, based on analysing their word choice and frequency in their e-mail data so as to determine the stress-related motives which could drive employees to commit a crime. However, their model could infringe upon the privacy of insiders, as they monitor e-mails and social media contents which might contain private information.

Kandias et al. (2010) proposed an insider prediction model based on capability, motivation, and opportunity which are elements of the Fraud Diamond. However, their model did not consider privacy issues and depended on information collected from insiders, which might not be reliable, as the insiders might have provided false information.

The model proposed in this research uses elements of the Fraud Diamond to detect suspicious insiders without collecting personal information to preserve their privacy, depending on factors such as resource usage behaviours, excluding contents and their interaction with honeytokens without identifying the insiders. The model also collects current information about insiders automatically using a context-aware system.

5.2.1.1 Motive

The model does not determine the motive but rather the probability that an insider is motivated to commit maleficence. It has been found in studies that insiders had been involved in stressful situations before committing a crime as a result of pressures from the organization or personal reasons. Organizational factors include dismissals, transfers, and denial of salary increases while the personal problems might be divorce, gambling and financial problems (Dhillon & Moores, 2001). Thus, detecting a change in the stress levels and emotions of insiders can be considered as a technique to predict insider threats.

Currently, cognitive and physical functions like stress are being currently monitored in clinical settings. Tools like the Mini-Mental State Examination (MMSE), the Abbreviated Mental Test (AMT) and the Mental Status Questionnaire (MSQ) are used for cognitive assessment while walking speed, joint range of motion and grip strength are used for physical assessment. Physiological measurements such as measuring the increase in stress-related hormones, heart rate and blood pressure, pupil dilation and galvanic response are used to measure stress (Goldberger & Breznitz, 2010). Affective computing, which measures the observable manifestation of emotions, is also used to detect stress. Automatic speech analysis has been used by Dinges, Venkataraman, McGlinchey and Metaxas (2007) to detect stress with an accuracy of 65%. Dinges et al. (2007) have

studied the pressure that is applied on during stressful situations and achieved an accuracy of 88% in detecting stress. However; the approach discussed above requires medical equipment to assess stress. These are costly items and could abuse the privacy of insiders, as it can also be used to assess symptoms of other diseases.

The use of typing patterns, together with techniques such as machine learning, timing and text features, has also been suggested by various authors to measure stress in addition to the security domain in which it is widely used (Dowland, Furnell & Papadaki, 2002; Khanna & Sasikumar, 2010; Villani, Tappert, Ngo, Simone, Fort & Cha, 2006; Vizser, Zhou & Sears, 2009). Various authors have recommended the use of keyboard interactions, as it is a simple technique to use and it does not require sophisticated hardware for monitoring. The reason is that cognitive and physical functions will depend on the current stress and health status of individuals (Araújo, Sucupira, Lizarraga, Ling & Yabu-Uti, 2005; Monrose & Rubin, 2000). Monrose and Rubin (2000) have found that the typing pattern of individuals is not stable and varies with their current stress and emotional levels.

Khanna and Sasikumar (2010) have also conducted an empirical study involving more than 300 participants. They report that most of the participants agree that when they experience a negative emotion, their rate of making a mistake will increase, followed by the use of the backspace and unrelated keys. Their typing speed will decrease. They also reported that the typing patterns of most of the participants were affected by their emotion based on their study using machine-learning techniques with an accuracy rate of up to 75% (Khanna & Sasikumar, 2010).

The model presented in this research also assesses the change in typing patterns, including the increase in the rate of mistakes and the decrease in typing speed to measure the stress levels of insiders. The model also assesses the rate of the use of negative words associated with stressed individuals, as some authors empirically postulated that stressed individuals used more negative words relative to normal employees (Khanna & Sasikumar, 2010). The typing pattern has been selected, as it does not require other medical devices for assessment and it does not infringe the privacy of insiders because it cannot be used to assess personal content.

An insider who is motivated to attack may also be detected using changes in resource usage behaviour in addition to his or her stress level; for instance, a searching behaviour of a normal user can be modeled to track any deviation from normal behaviour (Brown et al., 2013). Identifying insiders by using their resource usage behaviour, including file access, browser usage, process usage, downloading and file sending, is not new, for it has been investigated by several authors before (Maloof & Stephens, 2007; Sandhu, Coyne & Youman, 1996; Zhang, Chen, Shi, Xu & Pu (2014).

Chen, Nyemba and Malin (2012) proposed an approach which collected data on user activities and used K-nearest to see any deviation from normal activities. However, it only focused on anomalies and ignores abnormal activities. Zhang et al. (2014) proposed an architecture which studies both the individual's document access behaviour to detect any deviation, not only from individual behaviour but also from the community behaviour.

Ted et al. (2013) conducted applied research by "exploring and developing various algorithms for anomaly detection for insider threats, based on factors that included suspected scenarios of malicious insider behaviour, indicators of unusual activities, high-dimensional statistical patterns, temporal sequences and normal graph evolution" (p.1393). One of the algorithms investigated was Relational Pseudo-Anomaly Detection (RPAD) which was adopted for the model proposed in this research, as it is had resulted in very high-performance rates.

RPAD first learns a model of normal resource usage behaviour of a user, while considering it as non-anomalous. Then RPAD constructs equivalent numbers of pseudo-anomalies which deviate from the normal behaviour. RPAD will then construct a classifier to be used to classify a data instance as non-anomalous or pseudo-anomalous. To classify a new instance, RPAD uses both the decision of the classifier as well as pseudo-anomaly distribution to determine the instance as anonymous or not. According to their experiment, RPAD performs impressively, achieving an area under the curve (AUC) of 0.979 (Ted et al., 2013). "AUC directly estimates the probability that a randomly chosen positive entity extent will be ranked higher than a randomly chosen negative one" (Ted et al., 2013, p.1398).

This model has adopted changes in resource usage behaviours in addition to their stress level which is determined by the typing pattern as one element in detecting the motivation of insiders to commit a crime, as it does not collect any personal information.

5.2.1.2 Opportunity

Stoll (1988) was the first to introduce the concept of "honeypots". He attempted to create a false government project with the intention that intruders will access the files and analyse them for the purpose of committing a crime. Later, the term "honeypots" was coined by Spitzner (2003) who defined the term as a "… security resource whose value lies in being probed, attacked or compromised" (p.37). Anagnostakis, Sidiroglou, Akritidis, Xinidis, Markatos and Keromytis (2005) defined honeypots as a deception trap which is designed to appear like a legitimate system to fool attackers in their attempt to compromise the information system of an organization to serve as an early warning and advanced surveillance tool in minimizing the risk of IS crime.

Honeypots can be used at different levels of security measures, including prevention, detection, and reaction. Honeypots are very useful in uncovering the techniques and tools used by attackers to abuse information resources. Using this information, security practitioners can design a strong security system that outsmarts the tools and techniques used by intruders. It also helps to catch intruders while interacting with a honeypot.

There is a misconception about honeypots that people consider it to refer only to physical resources with which intruders will be motivated to interact in order to commit a crime. However, there is another instance of a honeypot which refers to digital information resources. This honeypot has been designed as a deception trap and is not a computer. The digital resource may be a credit card number, an Excel sheet that contains a password, a database entry and the like which are expected to attract an offender, however these are fake resources. These fake resources are termed *honeytokens*.

Though the term "honeytoken" is new to the information security field, the concept has been exercised in security for some time. For instance, some mapping agencies intentionally include fake cities and streets in their maps to check whether their

competitors copy their maps even without correcting the mistakes, which are literally a concept of honeytoken (Spitzner, 2003).

Honeypots have been used in the information security domain by various researchers. A number of studies have been conducted on using honeypots to detect the insider threat (Brown et al., 2009; McGrew, 2006; Padayachee, 2015). Cenys, Rainys, Radvilavius and Gotanin (2005) have developed three honeytoken modules and incorporated it into the DBMS Oracle 9i Enterprise Edition for the purpose of trapping intruders who attempt to attack information systems. Padayachee (2015a) employed honeypots to lure insiders to attack honeytokens and then her model intervened to remove any justifications/rationalizations the insider might use to attack the target by using the neutralization mitigation technique. Brown et al. (2009) have also used honeypots by producing a decoy document to detect any malicious activity by means of monitoring the interaction of insiders with the decoy document.

This model adopts honeytokens to lure insiders to commit a crime in order to assess whether insiders will use any opportunity to commit a crime. It is used based on consideration of privacy, as there is no personal information to be collected. The report of any interaction with honeytokens will not expose the identity of the individual to preserve his or her privacy.

5.2.1.3 Capability

Wood (2000) identified criteria which can be used to qualify a malicious insider. According to the author, there are two attributes to qualify an insider; these are knowledge and skills. The knowledge aspect is leveraged when an insider is familiar with the internal business of the organization or he/she can acquire the internal workings of the organization easily without any risk. Skills assume that an insider will have skills to launch an attack on a system because he or she is familiar with the organization.

The research model assumes that it is difficult for an insider to mount an attack on a system without having the requisite knowledge and skills. Neumann (1999) argues that the

knowledge and skills of an insider are very important factors for detecting and mitigating an insider threat problem. Magklaras and Furnell (2001) also underline the importance of considering the knowledge and skills of insiders to address the insider threat problem. These authors propose and insider threat prediction and prevention model based on various variables related to user characteristics which will be input to insider threat misuse estimate functions. The user characteristics include legitimate user attributes, depth of knowledge and fitness. Evans and Simkin (1989) have attempted to assess user sophistication of computer professionals, based on variables such as age, gender and other individual differences; however, their model is specific to computer professionals.

Huff, Munro and Marcolin (1992) propose a general model for user sophistication after interviewing users based on their experience with using information systems. Based on the results of their study, the authors proposed an end-user computing (EUC) sophistication model by classifying the users into three attributes:

Breadth of knowledge: Their study claims that advanced users are able to utilize many IT tools when compared to intermediate or novice users.

Depth of knowledge: Their research has found that the skills and knowledge acquired by training and practical experience are directly related to the level of user sophistication.

Finesse: This attribute refers to the ability of the user in solving IT problems to be one of the factors to be considered when measuring user sophistication.

The model presented in this research also uses the breadth of knowledge, depth of knowledge and finesse to assess the capability of insiders as these factors are related with the capability and skills of insiders.

Another important factor for capability is the role of the system insiders fulfill. According to instances of insider threats compiled by the CERT database (Cappelli et al., 2012), most of the crimes committed such as IT sabotage were executed by technically sophisticated IT professionals such as systems administrators exploiting the technology to harm an individual or organization directly.

The same pattern is seen in insider cases related to insider fraud, as most of the insiders who had participated in fraud were technically sophisticated employees. In one such case, a database administrator of an insurance company downloaded the personal information of its customers, including sensitive information about credit cards, to his removable media and he attempted to sell the personal information online to fraudsters. Therefore, the practical insider cases compiled by CERT require the consideration of systems roles in predicting and mitigating insider threat problems.

The idea of considering roles to address insider threat problems is not new, as it has been used by authors like Kandias et al. (2010) and Legg, Buckley, Goldsmith and Creese (2017). This model also considers the roles of insiders (novice, advanced, systems administrator) to assess their capability in protecting their privacy without identifying the individuals in the system. Zhang et al. (2014) argue that skillful employees usually carry out their activities effectively by using "pre-programmed" sequences of behaviours and they make fewer errors relative to unskilled employees unless they do it intentionally.

The number of errors that employees commit and the number of warnings they receive while using applications are factors that are also used to assess the capability of insiders as highly capable insiders make less errors compared to less capable insiders.

The model presented in this research assesses the capability of insiders to commit a planned attack based on their usage of computer applications measuring their sophistication in terms of "range of knowledge", "depth of knowledge" and "skill" as well as assessing the number of system errors and warning generated while using the applications.

5.2.2 Prevention

D'Arcy, Hovav and Galletta (2009) argue that user awareness and education about the organizational IS security policies is very important in preventing crime. Findings by Caputo, Maloof and Stephens (2009) indicate that "making employees aware of monitoring mechanisms, either through educational awareness or pop-up reminders,

could help deter malicious users" (p.20). Therefore, there is a need to educate at-risk users on the IS security policy of the organization. Prevention based on creating awareness will preserve the privacy of insiders, as it is possible to educate them electronically at run-time without identifying the individuals.

5.2.2.1 Rationalization

Insiders need to rationalize their criminal acts to avoid any guilt and excuse their criminal actions as per the Fraud Diamond. For instance, an insider may justify that he or she has been loyal to the organization for many years and it is justifiable to commit a minor crime occasionally.

One of the prevention strategies to mitigate insiders is to neutralize their rationalization, as insiders who think they may be detected and feel guilty are unlikely to commit the planned attack (Wells, 2008). As a strategy to neutralize any justification for crime, Sykes and Matza (1957) suggest five techniques, namely 'denial of responsibility', 'denial of injury', 'denial of the victim', 'condemnation of the condemners' and 'appeal to higher loyalties'. Minor (1981) added two more techniques, namely the 'metaphor of the ledger' and the 'defence of necessity' in addition to the five techniques proposed by Sykes and Matza (1957).

Siponen and Vance (2010) have studied the techniques proposed by Sykes and Matza (1957) and Minor (1981) to apply in the information systems security domain and confirmed that all of the techniques, except the denial of the victim, can be used for information security. This research implements the six neutralization techniques suggested by Siponen and Vance (2010) as prevention techniques for insider threats. These techniques are discussed below.

- *Denial of responsibility:* This technique refers to insiders who are not willing to assume any responsibility for their criminal acts, giving other excuses such as a large workload that lets them breach the IS security of the organization (Rogers & Buffalo, 1974; Sykes & Matza, 1957).

- *Denial of inquiry*: In this technique, the insider attempts to remove any guilt for his or her criminal action by providing justification that nobody will be affected negatively by the action (Siponen & Vance, 2010; Sykes & Matza, 1957).

- *Defence of necessity*: In this case, the insider rationalizes his or her crime by indicating that he or she has had no other option but to commit the crime (e.g. pilfering money to pay for rent in order to survive) (Piquero et al., 2005).

- *Condemnation of the condemners*: In this technique, the insider tries to blame other people for his/her criminal actions (Piquero et al., 2005). The insider may blame the manager who has forced the insider to commit an illegal act, fearing that he or she may be fired for not following orders.

- *Appeal to higher authorities*: In this case, the insider rationalizes that his or her criminal actions are justified, as it was done to accomplish very important work for the organization (Piquero et al., 2005).

- *The metaphor of the ledger*: In this technique, insiders justify that they have contributed a lot to the success of the organization and they reason that they should be excused for minor criminal actions (Klockars, 1974; Piquero et al., 2005).

The neutralization mitigation strategy will adopt the techniques suggested by the situational crime prevention theory, which are set rules (e.g. Information security policy and assist compliance (e.g. security education for staff)

5.2.2.2 Situational crime prevention (SCP)

According to Clarke (1983), situational crime prevention (SCP) can be defined as comprising measures directed at highly specific forms of crime that involve the management, design or manipulation of the immediate environment in as systematic and consistent a way as possible so as to reduce the opportunities for crime and increase the risks as perceived by a wide range of offenders.

Homel and Clarke (1997) argue that if offenders could be prevented from rationalizing and excusing their criminal acts, then they would be open to feelings of guilt and shame, which reduce crime. Cornish and Clarke (2003) propose five techniques for removing excuses, based on the situational crime prevention (SCP) theory. The theory includes set rules (e.g. harassment codes), post-instruction (e.g. “No Parking”), alert conscience (e.g. roadside display boards), assist compliance (e.g. Easy Library checkout), and control drugs and alcohol (e.g. alcohol-free events). Willison and Siponen (2009) propose two remove-excuse techniques, which can be used in the information security domain. These techniques are information security policy (set rules) and security education for staff (assist compliance).

The model proposed in this research uses SCP especially information security policy (set rules) and security education for staff (assist compliance) to nullify the excuses of insiders without identifying them individually to preserve their privacy. Nullifying excuses are used by insiders who attempt to use honeytokens without having authorizations to do so. It is assumed that insiders need to justify their criminal acts before committing a crime.

5.2.3 Privacy preservation

Privacy can be defined as a state where others do not access information about you without your consent (Moore, 1998). The right to privacy refers to the right of individuals to control any access to any personal information they do not want to disclose. According to a survey by Macworld (Branscomb, 1994) of 301 companies they have studied, 21% admitted that they searched employee files, including electronic work files in the order of 27% while 41% of the companies accessed the e-mails of employees, 27.7% accessed network messages, and the voicemail messages of employees were also accessed by 15.4% of the companies.

With the rapid increase in the use of technology in the workplace, employers are facing financial and legal challenges as a result of exposure to sensitive and confidential information like trade secrets. The misuse of online resources by employees may result in

legal action (Tabak & Smith, 2005). However, monitoring the online communication of employees has negative implications because it affects the privacy of insiders, and their personal information may be accessed by intruders when they are monitored online. The problem is aggravated by the fact that most employers consider workplace online communication to be used for work-related activities only and employees should not expect any privacy (Eivazi, 2011). Workplace monitoring may seriously damage the culture of mutual trust between the employers and employees (Eivazi, 2011). IT monitoring has other negative impacts, including abusing employees' expectation of privacy rights, fairness in negative judgments and effectiveness in work, and it may also result in stress-related illnesses (Rosenberg, 1999). Levinson (2010) argues that employees' privacy should be reserved during workplace monitoring and that there is a need to amend existing laws to support preserving the privacy of insiders.

This research model attempts to preserve insider privacy by collecting metadata only excluding contents such as search behaviour, file access, logins, using keystrokes and linguistic features without collecting the content to balance privacy issues as shown in Figure 5.1. The metadata will also be anonymized to protect the privacy of insiders. The opportunity facilitation and the neutralization mitigation will be deployed anonymously.

Anonymization

Anonymization of data can be achieved by means of the perturbative or the non-perturbative method (El Emam & Dankar, 2008). The perturbative method is implemented by adding noise and swapping data. However, this method is criticized because of its limitation to not preserve data truthfulness. For instance, the method may change the age of an insider from 45 to 15, whereas the non-perturbative method maintains the truthfulness of data. The researcher has adopted the former method for the model proposed in this study.

The perturbative method is widely implemented by making use of a technique called K-anonymity (El Emam & Dankar, 2008; El Emam, Dankar, Issa, Jonker, Amyot, Cogo,

Corriveau, Walker, Chowdhury, Vaillancourt and Roffey, 2009; Samarati, 2001) which will be discussed below.

K-anonymity

K-anonymization is a process of implementing K-anonymity, and it can be done by partitioning T into groups of at least k tuples, and then transforming the QID values in each group so that they become indistinguishable from one another (Gkoulalas-Divanis & Loukides, 2013).

We say K-anonymity is satisfied when each tuple in a table T (a1, . . . ,ad), where ai, i = 1, . . . ,m are quasi-identifiers (QIDs), is indistinguishable from at least k−1 other tuples in T w.r.t. the set {a1, . . . ,am} of QIDs (Gkoulalas-Divanis & Loukides, 2013). Quasi-identifiers are not unique identifiers by themselves but an intruder can combine different QIDs with the personal knowledge of the target and can uniquely identify the individual. Under this technique, it will be difficult to access the identity of insiders based on QIDs, as it will not be greater than 1k.The variable K will be assigned by the data owner, depending on the required privacy level. It is important to note that not all attributes in T need to be QIDs; m may be less than d, and it implies that an insider may not agree to be linked to any of those attributes.

5.3 The model

The model (depicted in Figure 5.1) is based on the Fraud Diamond which comprises four components: pressure (i.e. motive), opportunity, ability, and rationalization, as adopted from Kandias et al. (2010). According to the Fraud Diamond, fraudsters need to have motive and available opportunity to commit a crime. They should also have the capability to execute their planned attack. In addition, they need to justify or rationalize their criminal activities to become involved in crime.

The researcher significantly improved this limitation of the model proposed by Kandias et al. (2010) which is based on the components of the fraud triangle, namely capability, motivation, and opportunity. The first improvement of the model is that the researcher

has included one more element of the Fraud Diamond to the model, namely rationalization, a very important element to commit a crime in which requires insiders to justify their criminal activities to remove any excuse.

Kandias et al.'s (2010) model also does not have a privacy-preserving, as the collected data about motive and capability can be exploited by intruders. In addition, their model is limited to the prediction level while the model presented in this research has added a component of prevention strategies based on neutralization mitigation and the situational crime prevention technique.

Another limitation of Kandias et al.'s model (2010) is that it collects information about the motive and capability of the user, based on the questionnaire distributed to employees. This information may not be reliable, as employees may not be honest in providing accurate information and it does not have current information about the insider. Whereas the model proposed in this study contains a context-aware component which collects information about motive and capability at run-time, using their information resource usage behaviour such as file access, browser and process usage, typing pattern, errors and warnings. The model defined in this thesis was presented at an international conference (Mekonnen, Padayachee & Meshesha, 2015).

The model collects contextual information, using context analyser information about the motive and capability of insiders to detect any risk of committing maleficence. The current contextual information of the insiders is analysed by means of the context analyser. The context analyser assesses their motive, based on their resource usage behaviour such as their typing patterns, search behaviour, file access and logins without including personal contents to protect their privacy. The capability of insiders will be assessed in terms of the range of knowledge, breadth of knowledge and skills in using information resources as well as the number of errors and warnings generated while they are using an application. The number of errors and warnings is used to assess the capability with the assumption that users will produce fewer errors and warnings for an application in which they are skilled and with which they are familiar. Based on the contextual information, the model facilitates an opportunity to lure a high-risk insider to commit a crime by using a honeypot.

Based on the insider's reaction to the honeypot, the model will deploy an implementation strategy based on neutralization mitigation. An insider's reaction to the honeypot (i.e. clicking the honeytoken) activates neutralization mitigation. Neutralization mitigation is the process of removing the rationalizations that the insider may have had for committing the crime. Thereafter the model collects the rationalizations that the insider has used to attack information resources to use the rationalizations to remove any excuse for a crime as prevention technique. Situational crime prevention (SCP) techniques such as post-instruction (e-mail disclaimers), alert conscience (code of ethics) and assist compliance (hacker challenges) will be implemented to mitigate the threat. All of the information about insiders will be anonymized to remove any identifiers that may identify specific insiders so as to preserve their privacy.

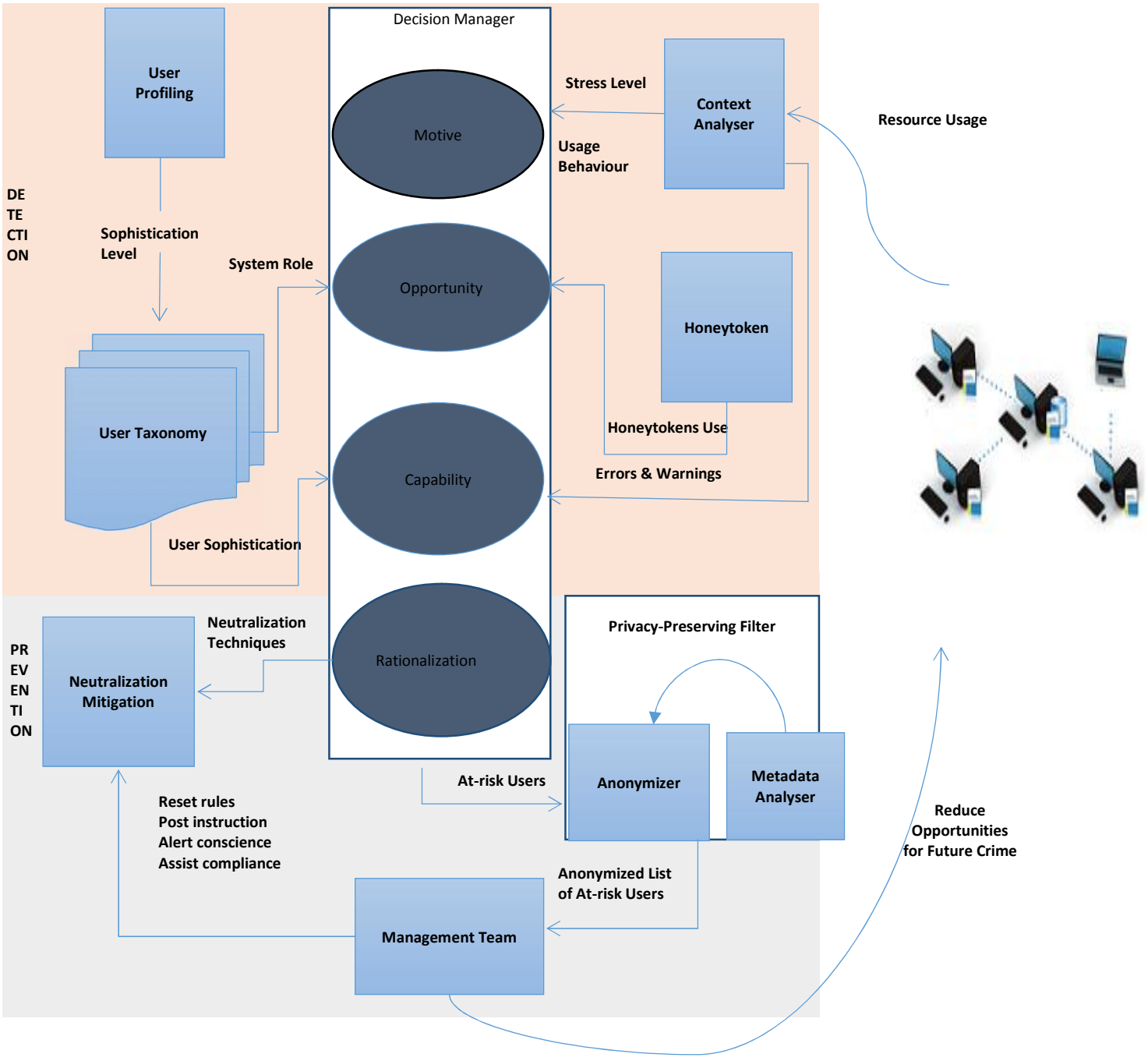

Figure 5.1 Privacy-preserving, context-aware, insider threat prediction and prevention model (adopted from Mekonnen et al., 2015)

Each component of the model is discussed in detail in the next sections.

5.3.1 Detection probability

5.3.1.1 Motive

The motive of an insider to commit a crime is assessed by collecting current information/contexts, using a component called the context analyser. This component only analyzes metadata and not any content that may contain personal information about the insider.

5.3.1.1a Component: Context Analyser

The context analyser predicts a high-risk insider based on the metadata collected about the activities of the insider. The metadata includes the insider's search behaviour, file access, logins, keystrokes and linguistic features without collecting the content to balance privacy issues (see Figure 5.2).

The context analyser assesses the typing pattern of the insider to determine his or her stress levels and emotions, which will be an input to assess his or her motive to commit a crime. The context analyser will also be used to analyse any change in the normal resource usage pattern such as the file access as well as browser and process usage to determine whether the insider has any motive to commit maleficence.

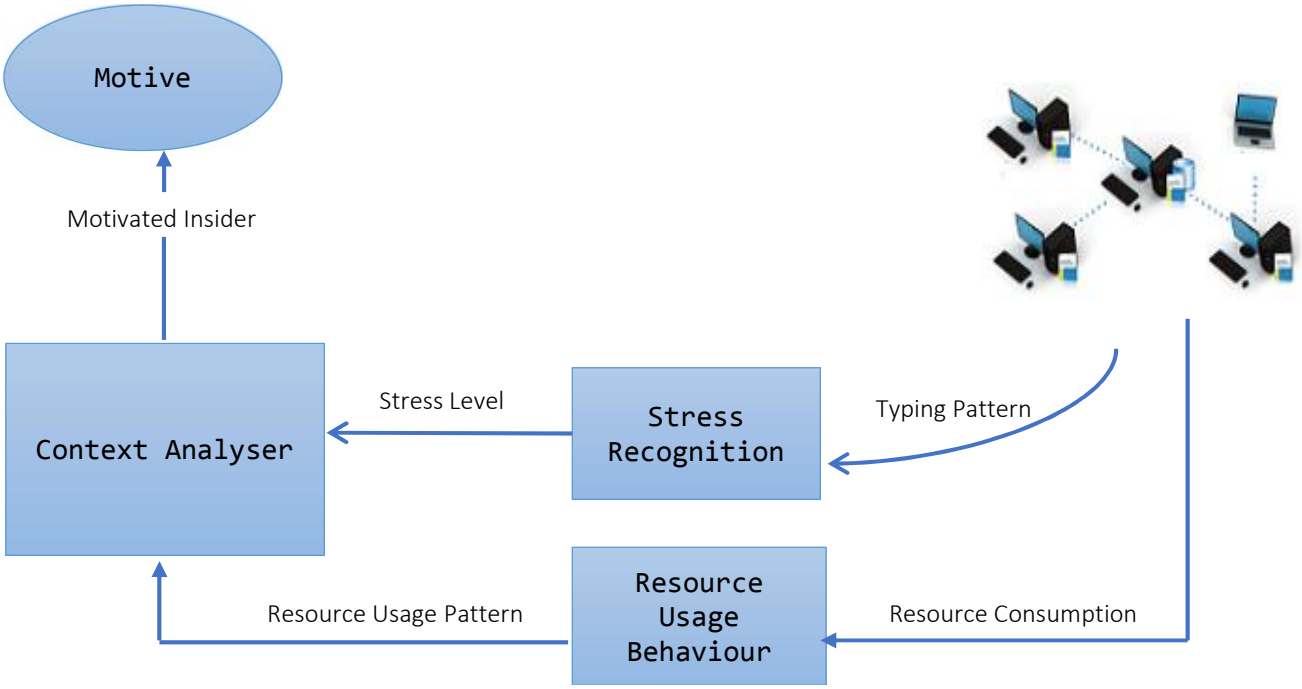

Figure 5.2 Context analyser

Stress recognition

The model ~~first~~ learns the typing pattern of the insider in terms of the rate of mistakes in typing, typing speed and the use of negative words by using machine-learning language, specifically k-Nearest Neighbor (kNN) as it has been applied with high accuracy by Khanna and Sasikumar (2010).

Then the current typing pattern is monitored and any change in the typing pattern is measured to assess the change in stress levels and emotions. These factors may motivate insiders to commit a crime which will be an input to their decision. The model has adopted all of the features for stress indications in the typing pattern of insiders, as suggested by Khanna and Sasikumar (2010) except some features like the negative affect rate which measures the use of negative words like *hate* and *fear*. These words are believed to infringe on the privacy of insiders. The features are presented in table 5.1.

Table 5.1 Timing, keystroke and linguistic features selected for analysis (adapted from Khanna and Sasikumar, 2010)

Feature	Definition
Pauth rate	Total # pauses/total # keystrokes. Pauses are defined as instances of no keyboard activity for over 0.5 s.
Pauth length	Total pause time/total # pauses. Pauses are defined as instances of no keyboard activity for over 0.5 s.
Time per keystroke	(Total input time – total pause time)/total # keystrokes. The adjusted time per keystroke excludes pause time.
Deletion keys rate	Total # delete keystrokes/total # keystrokes
Punctuation keys rate	Total # punctuation keystrokes/total # keystrokes
Other keys rate	Total # other keystrokes/total # keystrokes "m", "6" "Other" keys are those not counted in any of the above rates, such as letter and number keys.

The features presented in Table 5.1 determines the typing pattern of insiders. For instance, when an insider is under stress he/she might pause repeatedly while typing which will affect the pauth length and time per stroke. The insider might also commit various mistakes while typing during stress which will lead him/her to press the delete keys frequently which will, in turn, affect the deletion keys rate.

Resource usage behaviour

This part of the context analyser will determine the resource usage behaviour of insiders, including files access, browser usage, process usage, downloading and file sharing by

using a machine-learning algorithm, specifically k-Nearest Neighbor (kNN). Next, the model will measure any deviation from the normal resource usage behaviour of insiders to determine if there is any new motivation to attack information resources. The component also uses relational pseudo-anomaly detection (RPAD) model (Ted et al., 2013) to learn resource usage behaviour of a normal user, considering it as non-anomalous and then constructs equivalent numbers of pseudo-anomalies that will help to construct a classifier which will be used to categorize a data instance as non-anomalous or pseudo-anomalous.

5.3.1.2 Opportunity

Opportunity is one of the elements which facilitates a crime according to the Fraud Diamond. The model employs honeytokens as a means of evaluating insiders to determine whether they will exploit any opportunity to commit a crime without exposing any personal information about insiders to preserve their privacy.

5.3.1.2a Component: Honeytoken

This model uses honeytokens to determine whether the user will exploit any opportunity to commit a crime by making available fake information resources which an insider may wish to access, as shown in Figure 5.3.

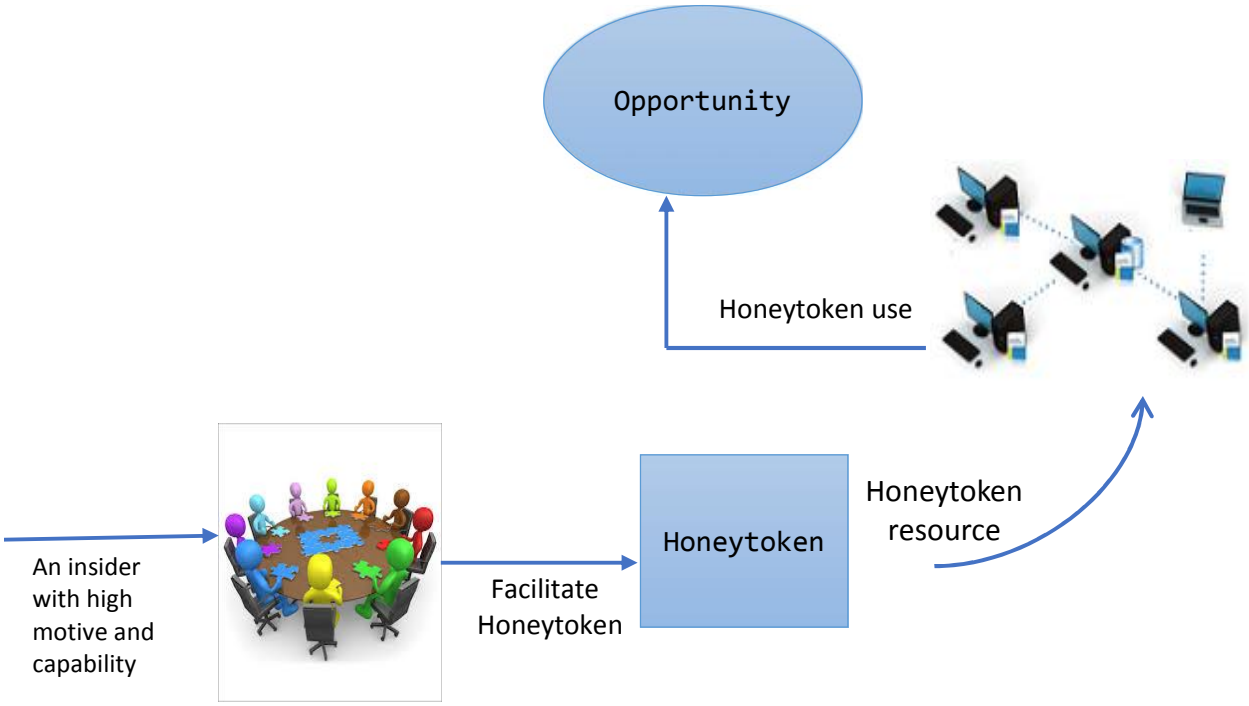

Figure 5.3 Honeytokens

The model will first identify an insider who may be motivated to commit a cybercrime based on his or her stress level and emotions. These aspects are assessed by the typing pattern as well as the change in resource usage behaviour. The model also assesses the capability of an insider to commit a planned attack based on his or her usage of computer applications by measuring the sophistication thereof in terms of range of knowledge, depth of knowledge and skill as well as assessing the number of systems errors and warnings generated while he or she has been using the applications.

The honeytoken will be facilitated by management to motivated and capable insiders only because there might be a risk of discouraging a loyal employee to feel that he/she is under surveillance. The honeytokens, which are fake information resources, will be used as deception traps to ascertain whether the insider will utilize an opportunity to commit a crime. The model will not use honeytokens to catch attackers and take legal action but rather educate the users who are at risk to become involved in a crime. This method is

believed to decrease any stress with workplace monitoring and also to balance the privacy issue.

5.3.1.3 Capability

The model will assess the capability of insiders to attack information resources based on three factors, namely their system role as determined by the organization, their sophistication level to be assessed while they use the information resources of the organization, and their user profiling in terms of the number of system errors they commit and warnings they receive while using the computational resources. The user sophistication will be assessed automatically without exposing the identity of individuals and will only be used to educate the users at risk of insider threat while protecting their privacy.

5.3.1.3a Component: User taxonomy

This component collects information about the systems role of the insiders as assigned by management and their sophistication levels in using the information systems of the organization. This component will be an input to assess the capability of the insiders to commit a crime.

The taxonomy is adopted from the insider threat prediction model developed by Kandias et al. (2010), as shown in Figure 5.4. It classifies users based on their systems role and level of sophistication.

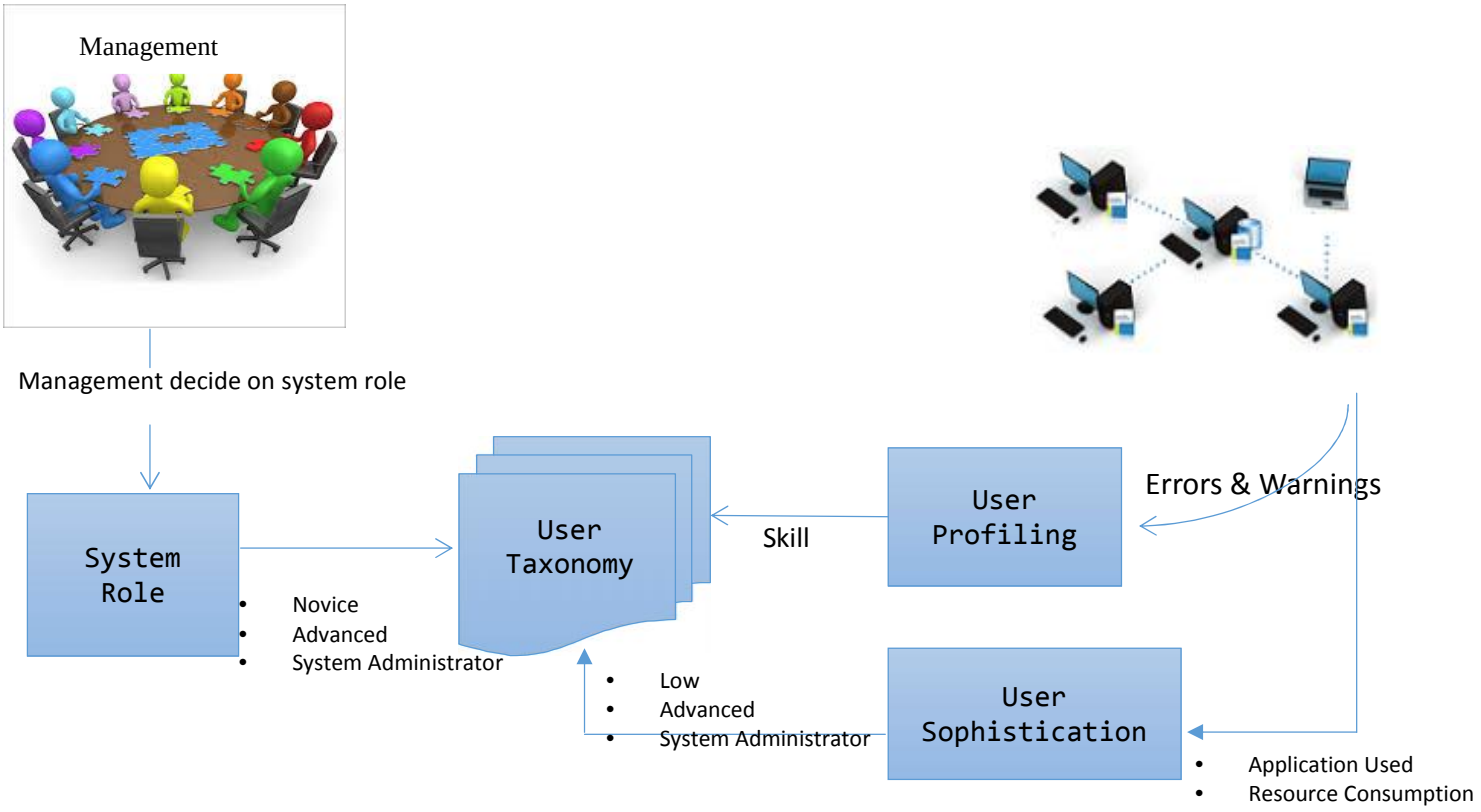

Figure 5.4 User taxonomy

Systems role

The model classifies employees into three roles which have also been used by Kandias et al. (2010). The roles will be assigned by the management team of the organization, depending on the job responsibilities of the employees. The classification is done with the intention of assessing the capability of the insiders of executing an attack plan, depending on the level of access right he/she is given by the management team of the organization.

This dimension classifies users into three classes (novice, advanced, administrator) based on the access right which management will grant them in advance.

Sophistication

This component automatically assesses the sophistication of insiders in terms of three factors. These are breadth of knowledge, depth of knowledge and finesse which focus on their use of information resources of the organization. The model adopts the following formula which has also been used effectively by Magklaras and Furnell (2005) and Huff et al. (1992) to measure user sophistication:

Fsophistication = Fbreadth + Fappscore + Fresutil

Fbreadth indicates how many different applications have been used, Fappscore indicates the user's sophistication regarding the type of applications he or she invokes and Fresutil represents the arithmetic sum of three computational resource consumption indicators (CPU, RAM, and simultaneous applications running).

Fappscore is calculated based on the following formula:

$$F_{appscore}=Score_{app1}+Score_{app2}+Score_{app3}+\ldots+Score_{appn} / n,$$

where n refers to the recorded number of applications for the user.

Freutil is measured using the following formula:

$$F_{resutil}=S_{CPU}+S_{RAM}+S_{SIMAPPS}$$

where S_{CPU} ***and*** S_{RAM} refer to the average consumption of CPU and RAM used by a user, while $S_{SIMAPPS}$ represents how many applications a user has utilized at the same time, based on the assumption that a highly sophisticated user will use many applications at a time relative to the average or novice user.

In order to calculate Fbreadth (breadth of knowledge), there is a need to measure the number of unique applications a user has used per session (avdiffapps). avdiffapps will be calculated with the following formula:

$$avdiffapps = \Sigma n_i/c, (i=1->i=c)$$

where n refers to the unique applications used by a user at a given session. For instance, if a user has opened four Microsoft Word documents, it will be counted as one unless the user is working on different applications. c represents the number of samples of user sessions that are used for the calculation in a given scenario.

To calculate Fbreadth, the following formula is used:

$$F_{breadth} = c_{high}, \text{ if } \mu_{ordinary} < x$$

$$F_{breadth} = c_{medium}, \text{ if } \mu_{novice} < x \leq \mu_{ordinary}$$

$$F_{breadth} = c_{low}, \text{ if } 0 < x \leq \mu_{novice},$$

where $c_{high} > c_{medium} > c_{low}$

where μ refers to the arithmetic average of *avdiffaps*

If μ represents the arithmetic average of *avdiffaps* for every user category and c is a pre-defined scoring constant associated with a particular user category, *Chigh* refers to the advanced user, *Cmedium* refers to ordinary user and *Clow* refers to a novice user. Finally, the result of sophistication is used to classify users as being at a low, medium or high sophistication level.

5.3.1.3b Component: User profiling

This component is used to assess the skill of the user which will also be used to determine the capability of the insider. The insider's skill is assessed based on the number of system errors he or she makes and the number of warnings he or she receives while using an application that he/she familiar with. The model considers other variables such as the number of errors and frequency in a short period. The errors and warnings are analysed, based on the assumption that the insider will generate fewer errors and warnings while using an application he/she are skilled to use and with which he/she is familiar.

5.3.1.4 Decision

The purpose of assessing the elements of the Fraud Diamond, namely motive, opportunity, capability and rationalization, is to detect any at-risk insiders and take preventive measures before the insider threat occurs. The model decides on the level of the risk the insiders hold for the organization, based on the assessment of motive, capability and opportunity as they have been assessed by other components of the model. The decision will not be communicated to the insiders and the information will be anonymized to preserve the privacy of the relevant insiders. The only purpose of the model is to educate the at-risk insiders on the information security policy of the organization so as to warn them of the risks when they plan on committing a crime.

5.3.1.4a Component: Decision manager

The decision manager will make an input based on motive, capability and opportunity from previous components, together with the user taxonomy as shown in Figure 5.5. The decision manager will then decide on the threat level of the insider, based on the algorithm adopted from Kandias et al. (2010).

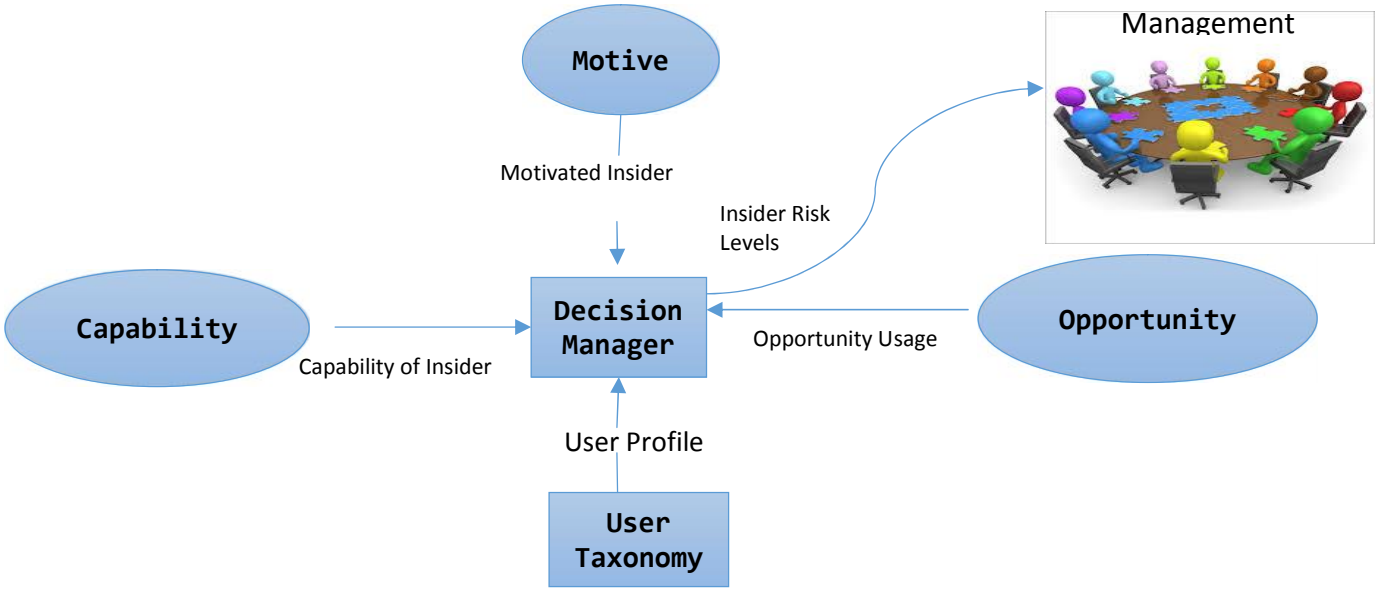

Figure 5.5 Decision manager

***Factor: Motive (Mi)*:** The motive of the insider is assessed by using the context analyser based on his or her typing pattern and resource usage behaviour. The insider's motive is ranked as low, medium or high.

Factor: Opportunity (Oi): The opportunity factor will be assessed based on the systems role assigned to the insider by the management (Ri) and his/her interaction with the honeytoken because the insider needs an opportunity to attack information resources. Therefore, the opportunity is a function of the role *Ri* and honeytoken use *Hi*:

$Oi = f(Ri,Hi)$

The first parameter, the user role as assigned by the management (*Ri*), could be that of a novice, advanced or administrator, as discussed in section 5.3.1.3. The systems role is important because user roles such those of as administrators can use their high privilege to commit a crime by creating a fake user and launching an attack through that user.

The second parameter is assessed based on the interaction of the insider with the honeytoken. The assessment of the opportunity element is demonstrated, using the scoring table as presented in Table 5.2.

Table 5.2 Opportunity score

Honeytoken use	**Systems role**		
	Novice	**Advanced**	**Administrator**
False	1	2	3
True	2	3	4
False	3	4	5
True	5	6	7

As is shown in Table 5.2, Opportunity score determined by usage of honeytoken by insider and their system role which will affect their ability to commit a crime if they are given an opportunity.

Factor: Capability (Ci): The capability element is assessed based on the user sophistication level and the skill level of the insider in terms of the number of errors and warnings generated. The insider's capability is ranked as low, medium, high or very high, depending on factors such as his or her competency in using the information system of the organization as well as his/her use of other computer resources (see section *5.3.1.3a*).

Decision algorithm

Once the decision manager receives input from other components on the ranking of the insider in terms of his/her motive (*Mi*), opportunity (*Oi*) and capability (*Ci*) a computation will be done to determine the risk level (*Ti*) of the insider. Three categories in this regard are low (1), medium (2) and high (3), as presented in Table 5.3.

$Ti = Mi + Oi + Ci$

Table 5.3 The overall threat score

Motive	**Opportunity**	**Capability**		
		Low	Medium	High
Low	Low	3	4	5
	Medium	3	5	6
	High	5	6	7
		Low	Medium	High
Medium	Low	4	5	6
	Medium	5	6	7
	High	6	7	8
		Low	Medium	High
High	Low	5	6	7
	Medium	6	7	8
	High	7	8	9

Note: Low=1, Medium = 2, High = 3.

It is proposed to further categorize the insider into four intervals by using four intervals, namely (3, 4), (5, 6), (7, 8) and (9) based on the insider's treat risk level which is calculated by adding their score for opportunity, capability, and motive. These numbers refer to the four categories: harmless, medium risk, dangerous and very dangerous respectively so as to give a detailed report about the insider. For instance, if user *i* is assessed as a user with high motivation (Mi = 3), high opportunity, (Oi = 3) and high capability (Ci = 3), then the threat score (Ti) will be 9 points, which will be reported as a very dangerous insider.

The assessment of the threat level of an insider will be an input for prevention strategies, as the insider who is considered a medium risk, dangerous or very dangerous should be mitigated by using neutralization mitigation and SCP with the support of the management team.

5.3.2 Prevention

Once the model, supported by the management team, decides on the risk level of the insider, the next step will be to take preventive measures. The prevention strategy proposed in this model is based on preserving the privacy of the insider. Thus, the model will not expose the decision about at-risk insiders, and all the data will be anonymized to preserve the privacy of the insider.

The prevention strategy is based on educating the insider to nullify any rationalizations to commit a crime by making use of neutralization mitigation and situational crime prevention techniques. The neutralization mitigation techniques include denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and appeal to higher authorities, the metaphor of the ledger and the defence of necessity.

The model uses information security policy (set rules) and security education for staff (assist compliance), alert conscience and assist compliance as they apply to the situational crime prevention technique.

5.3.2.1 Component: Neutralization mitigation

The neutralization component will be used to remove any justification for committing maleficence once it is proven that the insider will exploit any opportunity to commit a crime, depending on his or her interaction with honeytokens, as shown in Figure 5.6.

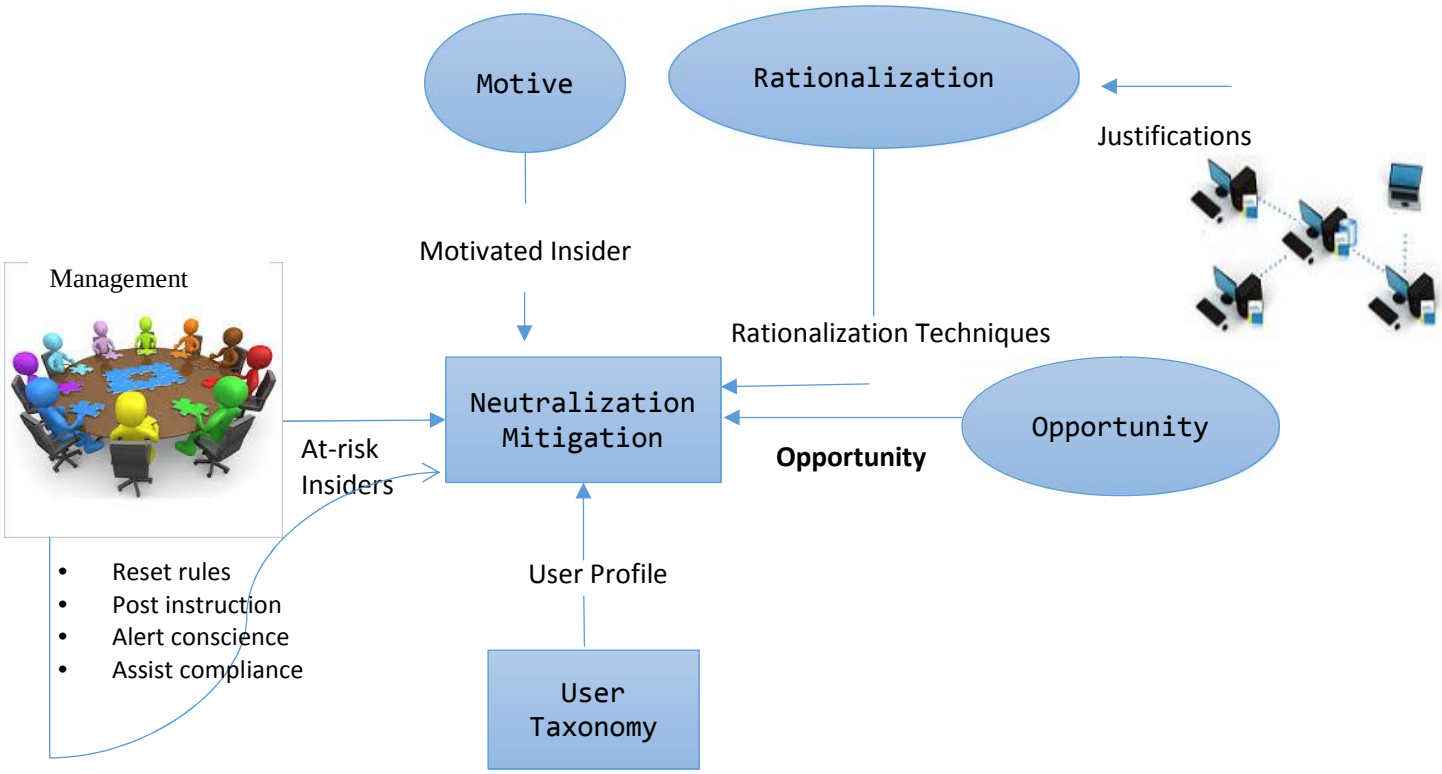

Figure 5.6 Neutralization mitigation

The model implements six techniques of neutralization mitigation suggested by Siponen and Vance (2010) to remove any justifications for crime in the information security domain. They are denial of responsibility, denial of inquiry, defence of necessity, condemnation of the condemners, appeal to higher authorities and the metaphor of the ledger.

These components will alert the at-risk insider about the information security policy which has been assessed by the neutralization techniques discussed above. It also provides the management team with an input to help them reset the rules based on the neutralization techniques which may be used to remove an excuse from the insider for committing a future crime.

5.3.2.2 Change management

In the final analysis, the management team will analyse all information gathered and computed by using different components of the model as inputs to design future strategies for insider mitigation. However, they will not be able to identify the high-risk individuals personally to preserve their privacy. Though it will be challenging to control the motive and the capability of the insider, the management team can work to minimize any opportunity that facilitates crime and remove any rationalizations to commit a crime.

In the model presented in this research, the techniques of SCP are suggested to remove any excuse for committing a crime in order to support the change management. The model uses five techniques proposed by Cornish and Clarke (2003) for removing excuses. They are:

1) set rules (e.g. harassment code) – the equivalent for the IS security domain may include policies, agreements, and procedures
2) post-instruction (e.g. “No Parking” notices) – the equivalent for the IS security domain is e-mail disclaimers (Beebe & Rao, 2005)
3) alert conscience (e.g. roadside display boards) – the equivalent for the IS security domain include a code of ethics (Coles-Kemp & Theoharidou, 2010)
4) assist compliance (e.g. Easy Library check-out) – the equivalent for the IS security domain include providing online help with information security policy (Willison, 2006)
5) control drugs and alcohol (e.g. alcohol-free events). However; drugs and alcohol are outside the information security domain

5.3.3 Privacy preservation

The model attempts to preserve the privacy of insiders by collecting metadata only, excluding contents such as search behaviour, file access, logins, using keystrokes and linguistic features without collecting the content to balance privacy issues, as shown in Figure 5.7. The metadata will be anonymized to protect the privacy of the insiders.

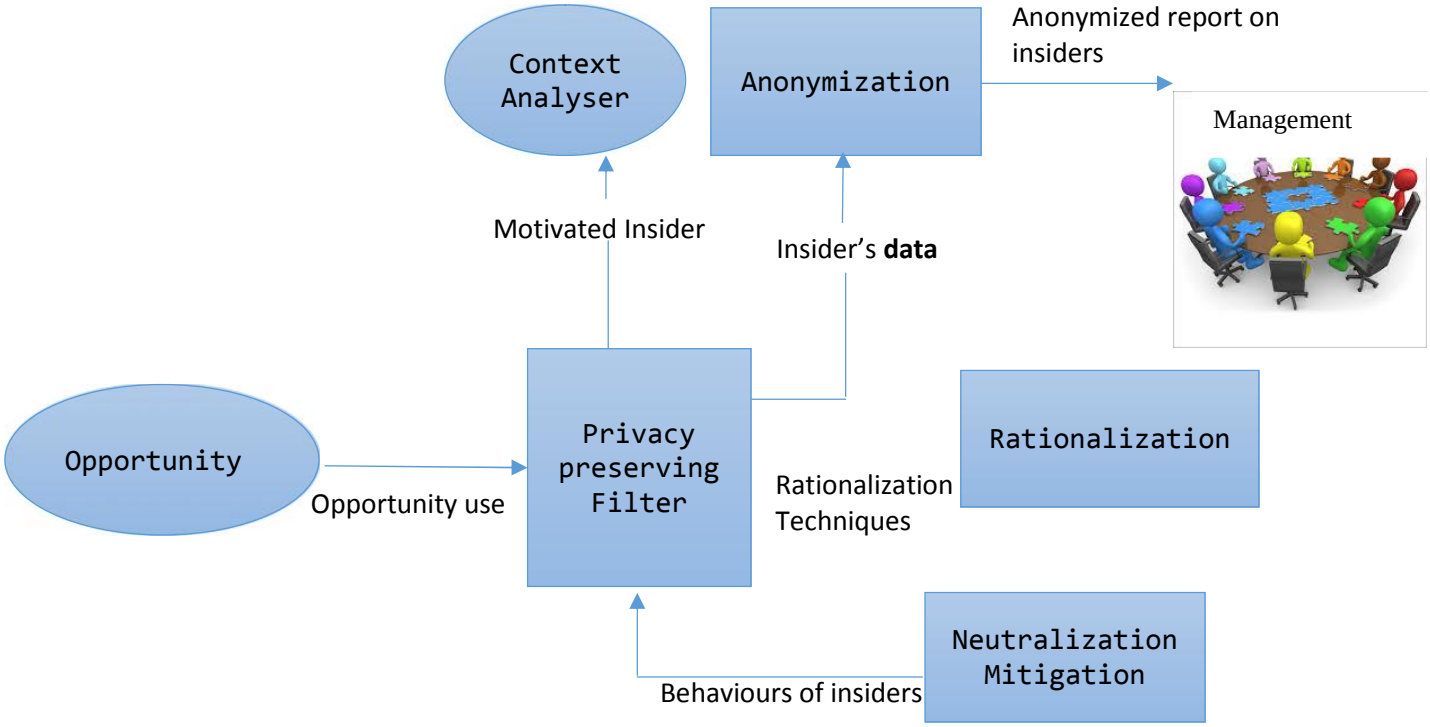

Figure 5.7 Privacy-preserving filter

All information collected by the model related to motive, capability, opportunity, and rationalizations will be anonymized (i.e. removing identifiers) with technique K-anonymization to preserve the privacy of insiders. k-Anonymization is the process in which a table T(a1, . . . ,ad), where ai, i = 1, . . . ,m are quasi-identifiers (QIDs), is

partitioned into groups {g1, . . . ,gh} s.t. |gj| ≥ k, j = 1, . . . ,h, where |gj| denotes the size of gj (i.e. a number of tuples contained in gj), and tuples in each gj are made identical with reference to QIDs (Gkoulalas-Divanis & Loukides, 2013).

The following three tables illustrate how k-anonymization works. Table 5.4 depicts the raw data with an identifier of staff ID from which it is easy to identify an individual from the ID which may be used by intruders.

Table 5.4 Original insider data

Serial Number	**Staff ID**	**Motive**	**Capability**	**Honeytoken use**
1	AAU/2567	High	Medium	Yes
2	AAU/1234	Medium	High	No
3	AAU/3489	Medium	High	No
4	AAU/4567	High	High	No
5	AAU/1910	High	Medium	No
6	AAU/2178	Medium	High	Yes
7	AAU/2956	Medium	High	Yes
8	AAU/5946	High	Medium	No
9	AAU/9234	Medium	High	Yes

There are two ways to anonymize this data. The first replaces the whole ID with another character which is completely secure (see Table 5.5) and the second replaces parts of the ID by other characters (see Table 5.6). It may be easy to rebuild the data; however, it is not completely secure because intruders may still attempt to identify the insiders from parts of their ID numbers.

Table 5.5 A3 - Anonymous version of table 5.4

Serial Number	Staff ID	Motive	Capability	Honeytoken use
1	*	High	Medium	Yes
2	*	Medium	High	No
3	*	Medium	High	No
4	*	High	High	No
5	*	High	Medium	No
6	*	Medium	High	Yes
7	*	Medium	High	Yes
8	*	High	Medium	No
9	*	Medium	High	Yes

As shown in Table 5.5, the staff ID is completely replaced (*) to make it completely secure and therefore, it is impossible for intruders to identify the particular insiders.

Table 5.6 A3 - Anonymous version II of table 5.4

Serial Number	ID	Motive	Capability	Honeytoken use
1	AAU/25**	High	Medium	Yes
2	AAU/12**	Medium	High	No
3	AAU/34**	Medium	High	No
4	AAU/45**	High	High	No
5	AAU/19*the*	High	Medium	No
6	AAU/21**	Medium	High	Yes
7	AAU/29**	Medium	High	Yes
8	AAU/59**	High	Medium	No
9	AAU/92**	Medium	High	Yes

In the anonymization presented in Table 5.6, parts of the staff ID were replaced; for instance, AAU/2567 changed to AAU/25**, replacing the last two characters with **. However, the information is not completely secure, as intruders can still guess who the individual is from the parts of his or her ID although it helps to easily rebuild the data.

5.4 Comparison to similar models

There are three other models and frameworks that are comparative to this privacy-preserving, context-aware, insider threat prediction and prevention (PPCAITPP) model which also deal with the insider threat problem. The comparison of PPCAITPP with these similar models is discussed next to illustrate the differences among the four models.

PPCAITPP and the Insider Threat Prediction model (Kandias et al., 2010)

Kandias et al. (2010) have proposed a model based on the three elements of the Fraud Diamond, namely capability, motivation, and opportunity. One of the differences in PPCAITPP, the model proposed in this study, is that it includes one more element of the Fraud Diamond, namely rationalization. This is another very important element to commit a crime.

The model proposed by Kandias et al. (2010) does not contain a privacy-preserving feature to preserve the privacy of an insider, as the information collected concerning the motive and capability of the insider may be exploited by intruders. In addition, their model is limited to the prediction level while the PPCAITPP model contains a component for prevention strategies, a very important component for insider threat mitigation.

Moreover, their model collects information about the motive and capability of the insider, based on the questionnaire distributed to employees. However, the information is not reliable, as employees might not be honest in providing accurate information. On the other hand, the PPCAITPP model includes a context-aware component, which collects information about motive and capability at run-time by using the insider's information resource usage behaviour such as file access, browser usage, process usage, typing pattern, errors, and warnings which are used in the model.

PPCAITPP and Predicting Insider Threat Risks Through Linguistic Analysis of Electronic Communication (Brown et al., 2013)

Brown et al. (2013) proposed a model to predict insiders based on their electronic communication such as their word usage in their e-mails and the social media so as to identify psychological indicators of potential insider abuse. Their approach is criticized for not preserving the privacy of insiders, as their model monitors the contents of the communication of insiders which is an abuse of their privacy. The model proposed in this research uses a metadata analyser to predict a high-risk insider based on metadata such as

search behaviour, file access, logins, the use of keystrokes and linguistic features without collecting the content to balance privacy issues.

Their model is also limited in predicting the motive of an insider, excluding other factors for committing a crime, namely opportunity, capability and rationalization.

In addition, their model focuses on the prediction level and does not consider the prevention aspect like the model proposed in this study does.

PPCAITPP and the Context-Aware, Insider Threat Prediction model (Memory, Goldberg & Senator, 2013)

Memory, Goldberg and Senator (2013) have proposed a model to predict insiders, based on the automatic collection of contextual information about the insiders' computer usage such as resources and devices used, networks and communication patterns.

Their approach emphasizes the collection of contextual information relative only to the motive of insiders and does not consider other factors for insider crimes such as opportunity, capability, and rationalization. The contextual information may be abused by intruders and the privacy of insiders is not be preserved. The model presented in this study has anonymized (removed identifiers) all contextual information to preserve the privacy of insiders.

Their model is also limited to the prediction level and does not address the prevention of crimes once the risk of insiders has been predicted.

5.5 Chapter summary

This chapter firstly discussed the overview of the model, describing how the components of the model worked together to predict and prevent insider threats while preserving the privacy of insiders (see section 5.1). Secondly, the derivation of the model was discussed in detail with the support of literature as well as with examples where required (see

section 5.2). Thereafter all components of the model were discussed in detail (see section 5.3). These components were based on prior research from the disciplines of criminology and computer science literature, which was believed to address the insider threat problem. Finally, the model was compared with similar approaches, which attempted to address the insider threat problem (see section 5.4). The comparisons showed that the model presented in this study addressed some of the limitations of current insider threat prediction and prevention models, especially regarding privacy preservation, the integration of different approaches, the use of context-aware systems to collect reliable and current information and proposing a comprehensive model, which predicts and prevents insider threats.

The evaluation of the PPCAITPP model will be discussed in the next chapter.

CHAPTER SIX

EVALUATION: CYCLE I

6.1 Introduction

Scientific rigor requires the evaluation of the artefacts based on the research goals specified and the methods chosen for the research (Österle et al., 2011). In design science research, there are different techniques proposed to validate an artefact, namely laboratory prototypes, simulation procedures, expert reviews and field experiments (Österle et al., 2011).

This chapter firstly discusses a prototype and simulations that have been used to demonstrate the artefact; in this study, it is a privacy-preserving, context-aware, insider threat prediction and prevention model using an asset management system as a case study.

Thereafter the chapter presents and analyses the feedback of a panel of experts who have evaluated the model in the first iteration, based on design science research principles. Finally, the findings will be discussed.

6.2 Prototype – Asset management system

To demonstrate the model using an application, an asset management system has been selected as a case study. The system is used to manage assets of an organization, starting from asset requisition requests until the use of an asset service ends. In the system, ordinary employees will fill online asset requisition forms to order an asset purchase which has to be authorized by department managers who then have to send it to the suppliers. The supplier will then supply the asset to the store clerk and the managers need to authorize the supply. After this has been done, the employees will request the asset for use and once it has been authorized by the managers, the store clerk will deliver the asset

to the employees. The system also manages any request for transfer of assets from among employees however it has to be authorized by managers. It maintains data about the depreciation of assets. Finally, once the asset is depreciated fully or if employees would like to return the asset to the store, the system manages that operation. There is some risk for the system to be abused unless there is a proper information security system in place. The reason is that intruders or insiders can authorize any asset purchase, transfer or delivery on behalf of the managers which will incur financial losses for the organization.

6.2.1 Modelling the prototype

Unified Modelling Language (UML) is used to visually specify and construct the concepts implemented in the prototype. Class diagram, use case diagram and activity diagram are used, and these aspects are discussed in the next section.

6.2.1.1 Class diagram

Class diagrams are used to describe the set of objects which have common attributes, operations, relationships and semantics, as per the guideline of the UML standard. Six classes are identified, namely Manager, Operational Employee, Insider, Order Details, Item and Suppliers.

The class manager contains attributes, which describe the manager (ID, name, age, etc.) as well his/her operation (authorizing purchase, transfer, etc.). The class operational employee is used to hold data about operational employees, including their ID numbers, names, addresses etc. and about the tasks they perform in the system such as requesting purchases, transfers and receiving material.

The data about insiders will be maintained by the *Insider* class. This data covers motive, capability, opportunity as well as operations such as using honeytokens and learning new behaviours. Data and operations about assets ordered by employees will be handled by class *Order details* and the data about assets will be maintained by the class *Item*. The

attributes and operations of the classes, as well as their interconnections, are presented in Figure 6.1.

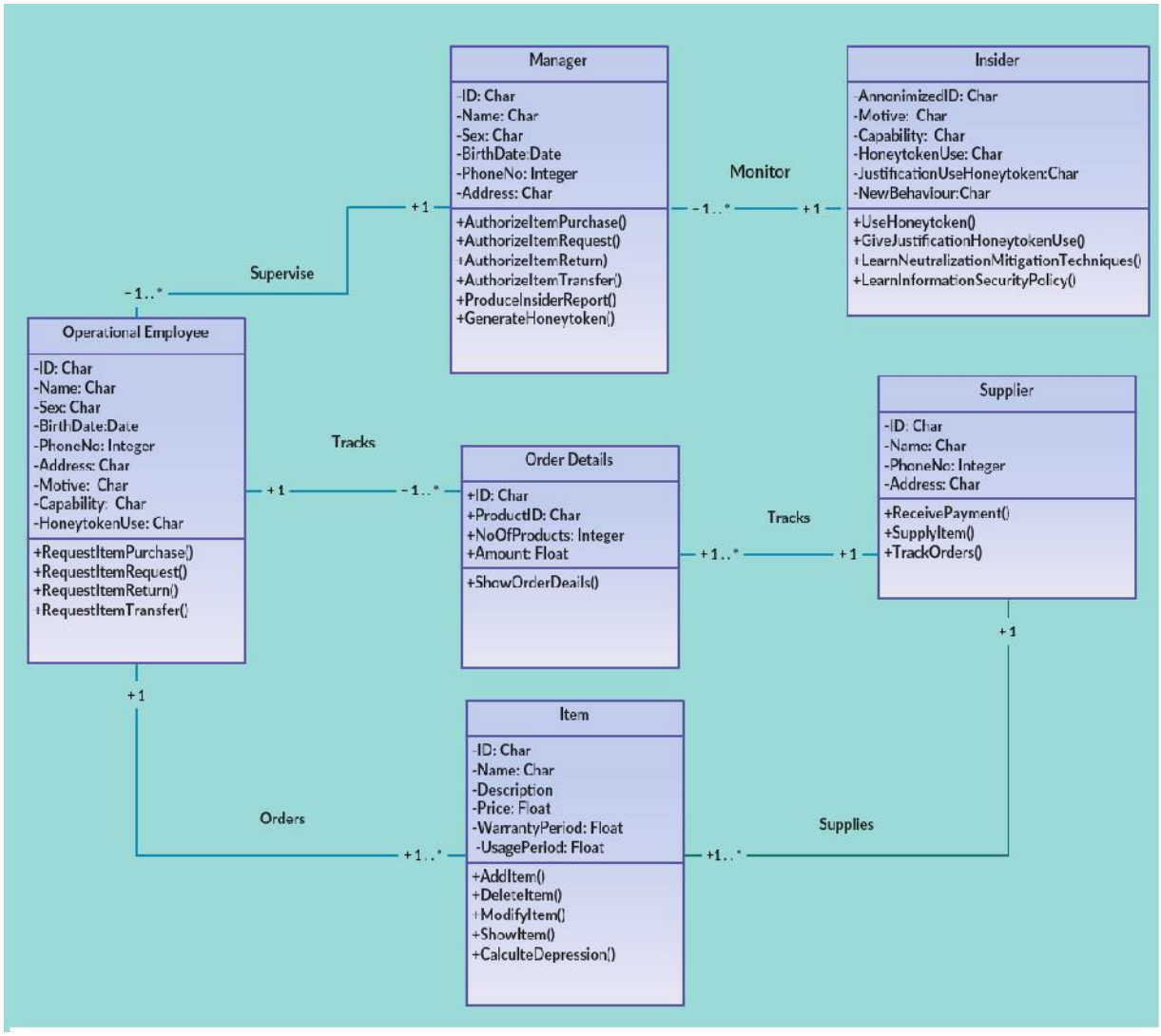

Figure 6.1 Class diagram of the prototype

6.2.1.2 Use case diagram

Use case diagrams are used to depict the sequence of actions in the prototype with which an actor interacts with components of the system to give the result to users according to the standard of UML. Five actors are represented in the diagram. They are *Manager*, *Operational Employee*, *Insider*, *Order Details*, *Item*, *Store Clerk* and *Suppliers*. All of the

use cases are represented in an eclipse form. The interactions between the actors and the use cases are represented by using a line and descriptions. The use case is presented in Figure 6.2.

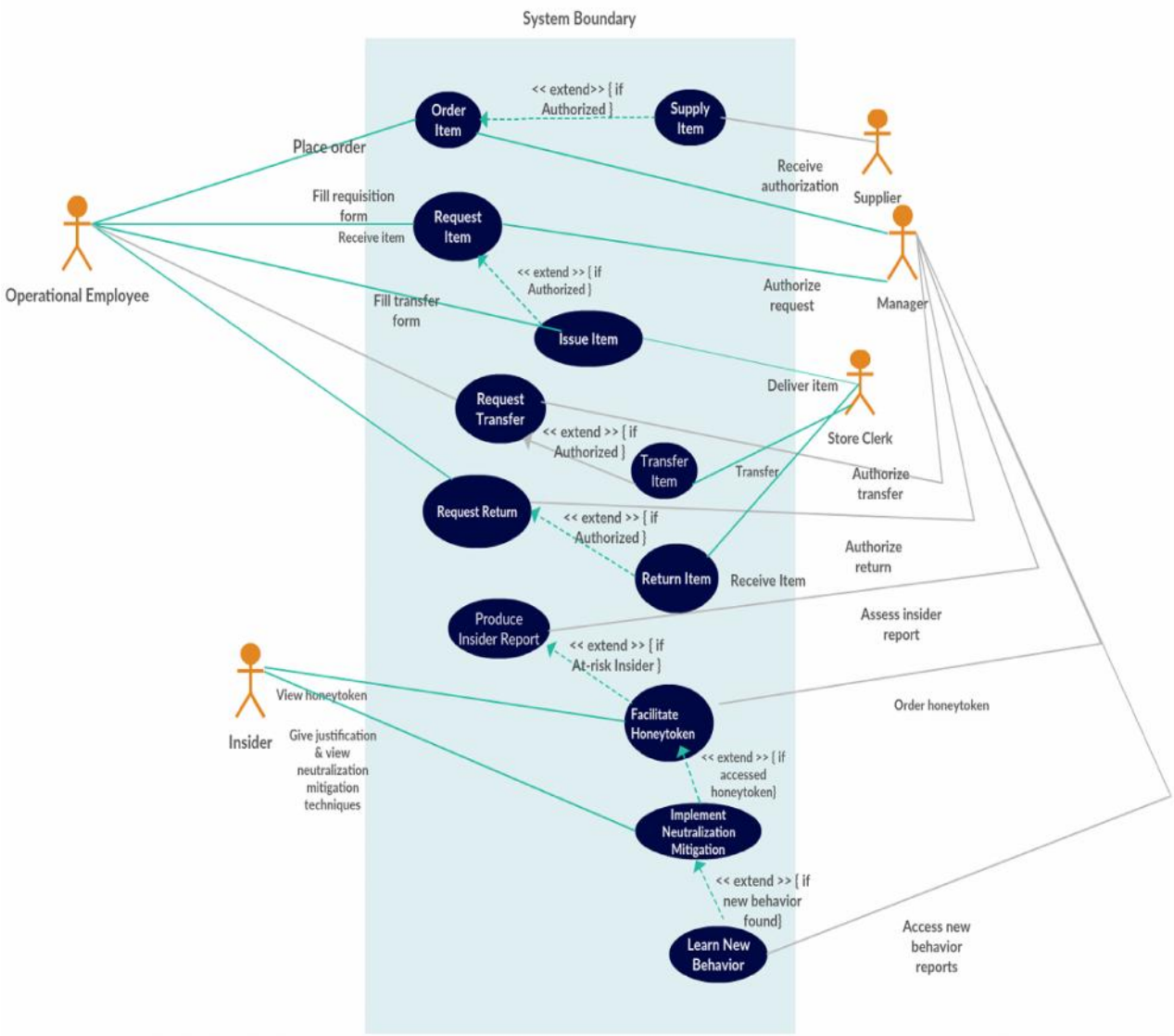

Figure 6.2 Use case diagram of the prototype

As shown in Figure 6.2, the actor *Operation Employee* places an order to acquire an asset, receives it after purchase and transfers it to another person as it is required. The *Store Clerk* actor is responsible to receive assets from suppliers and deliver them to operational employees. If the *Operational Employee* is projected to be a high-risk insider,

he/she would also be lured to access a honeytoken, and if he/she did, he/she would be asked to provide justification for accessing the honeytoken without authorization.

The actor *Supplier* is the one who delivers the asset once it is authorized by the managers. The actor *Manager* is responsible to authorize the item purchase, delivery and transfer as well as decide to facilitate the honeytoken for the suspected insider. He or she will also receive reports about the insider.

6.2.1.3 Activity diagram

To describe the operational workflow of the prototype using UML standard, an activity diagram is drawn which is presented in Figure 6.3.

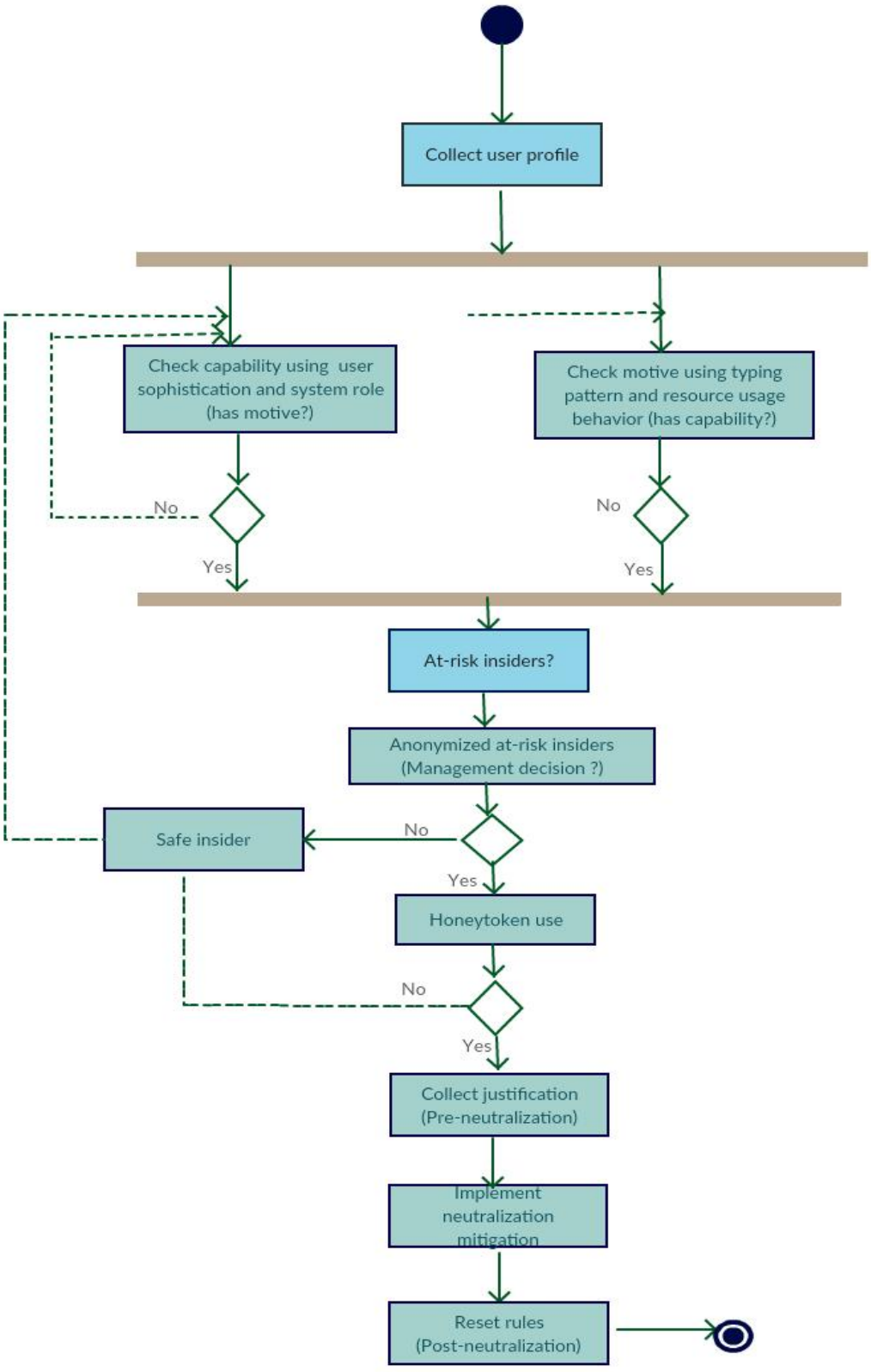

Figure 6.3 Activity diagram of the prototype

As shown in Figure 6.3, the system assesses capability in terms of user sophistication and systems role as well as motive by using the typing pattern and resource usage behaviour of the insider. If the insider has the motive and the capability to commit a crime, he or she will be considered an at-risk insider; otherwise, the assessment will continue.

The data about at-risk insiders will be anonymized to preserve their privacy. The management team will view the anonymized data to decide whether they really are high-risk insiders. If the management team confirms their risk, they will facilitate a honeytoken to check whether the insiders will use an opportunity to commit maleficence. Otherwise, they will be considered safe insiders.

If the insiders accessed the honeytoken without authorization, they would be asked their rationalization for committing a crime after which the neutralization mitigation technique will be implemented to remove any rationalization the insiders might use to commit a crime. Finally, based on the insiders' data, the management team will reset the rules so as to prevent similar crimes in the future.

6.2.2 The proof of concept

To demonstrate the model concept, a proof of concept/prototype has been developed, taking the asset management system as a case study because insiders usually abuse the information system at the application level. The system is demonstrated by using an interface prototype. Functional prototypes have also been developed for some parts of the model. A simulation has been developed for the typing pattern of the context analyser and for the anonymization part of the privacy-preserving filter.

The prototype has five components: *report on anonymized at-risk insiders, honeytoken generator, neutralization mitigator, reporting on an anonymized report on the behaviour of insiders* and *stress detector*.

In the case study, there are two types of users with different privileges. The first type of user is a normal user who will check the status of items such as whether they have been requested, purchased or transferred and what their availability in the store is. The second

type of user has a managerial privilege. He or she will authorize the purchase, transfer, and distribution of items.

The manager will be able to access the reports about insiders. These reports include a list of anonymized at-risk insiders as well as an anonymized report on the behaviour of insiders.

The prototype firstly assesses the *capability* and the *motive* of insiders in order to be able to predict any at-risk insiders. The *capability* factors will be assessed by *user sophistication* and the *user profiling component*. The *user sophistication* is assessed based on three factors, namely *breadth of knowledge, depth of knowledge* and *skill*. The *user sophistication* component is hardcoded to demonstrate how it works. The *user profiling* component will use metadata such as the *number of errors* and *warning messages* generated by the user while using an application with which the insider is familiar to assess his/her sophistication level.

The motive of the user is assessed in terms of his/her usage behaviour, including typing pattern behaviour, file access, and browser usage. As part of the prototype, a typing pattern analyser has been implemented for checking the typing speed and the number of errors the user makes while using a specific application with which he/she is familiar. Literature has found that the typing speed and the number of errors change when people find themselves in stressful situations. It has been found that most insiders have been in stressful situations before committing a crime.

Finally, the prototype will prepare a report on the list of at-risk insiders based on the assessment of their motive and capability. This report is anonymized (with no identifiers) to preserve their privacy. A sample report is presented in Figure 6.4.

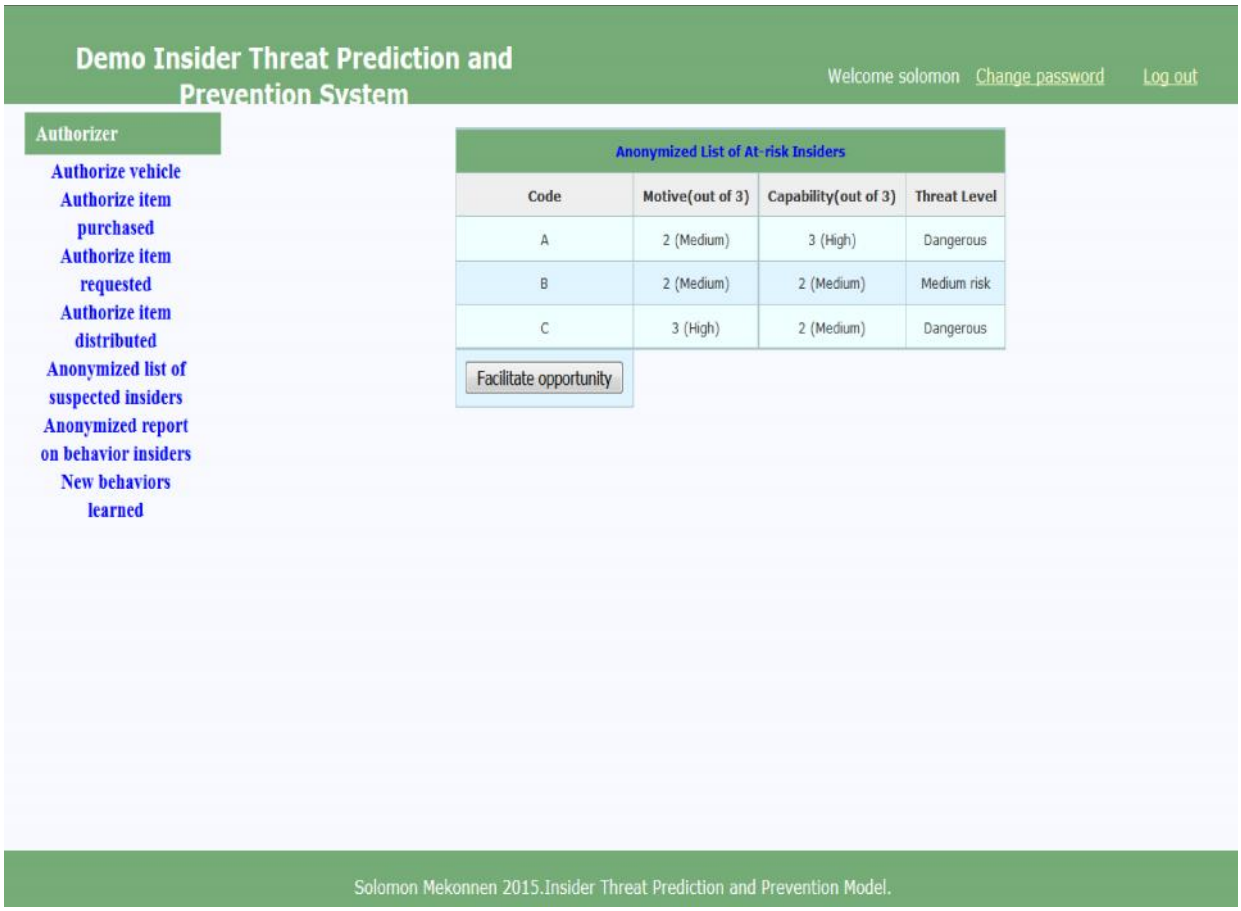

Figure 6.4 Interface: Anonymized list of at-risk insiders

The report depicts the motive of insiders as low, medium or high, based on the assessment of their typing patterns and resource usage behaviour. It also displays the capability of insiders as low, medium or high to commit a crime, based on their sophistication levels and systems roles. It also computes their threat level as low risk, medium risk or dangerous risk, based on their capability and motive. The report is anonymized with no identifiers.

The management team will review the report and decide whether to facilitate a honeytoken to the insiders based on their risk levels or not. The manager will also assess the report of the at-risk insiders and decide whether to facilitate an opportunity by using honeytokens to lure the insiders to commit a crime. If the manager is convinced that he/she should facilitate the honeytokens, the system will make available an extraneous

link, *Authorize*, to the at-risk insiders to lure them to be involved in authorizing items for purchase or transfer or distribution which fall outside their authorization permission. The extraneous link is presented in Figure 6.5.

Figure 6.5 Interface: Extraneous link as a honeytoken

When the insiders click on the *Authorize* link, they will be provided with a pre-neutralization mitigation warning, which falls outside of their authorization, to authorize items in an attempt to alert their conscience. The insiders will then be asked whether they wanted to access the service. The warning is shown in Figure 6.6.

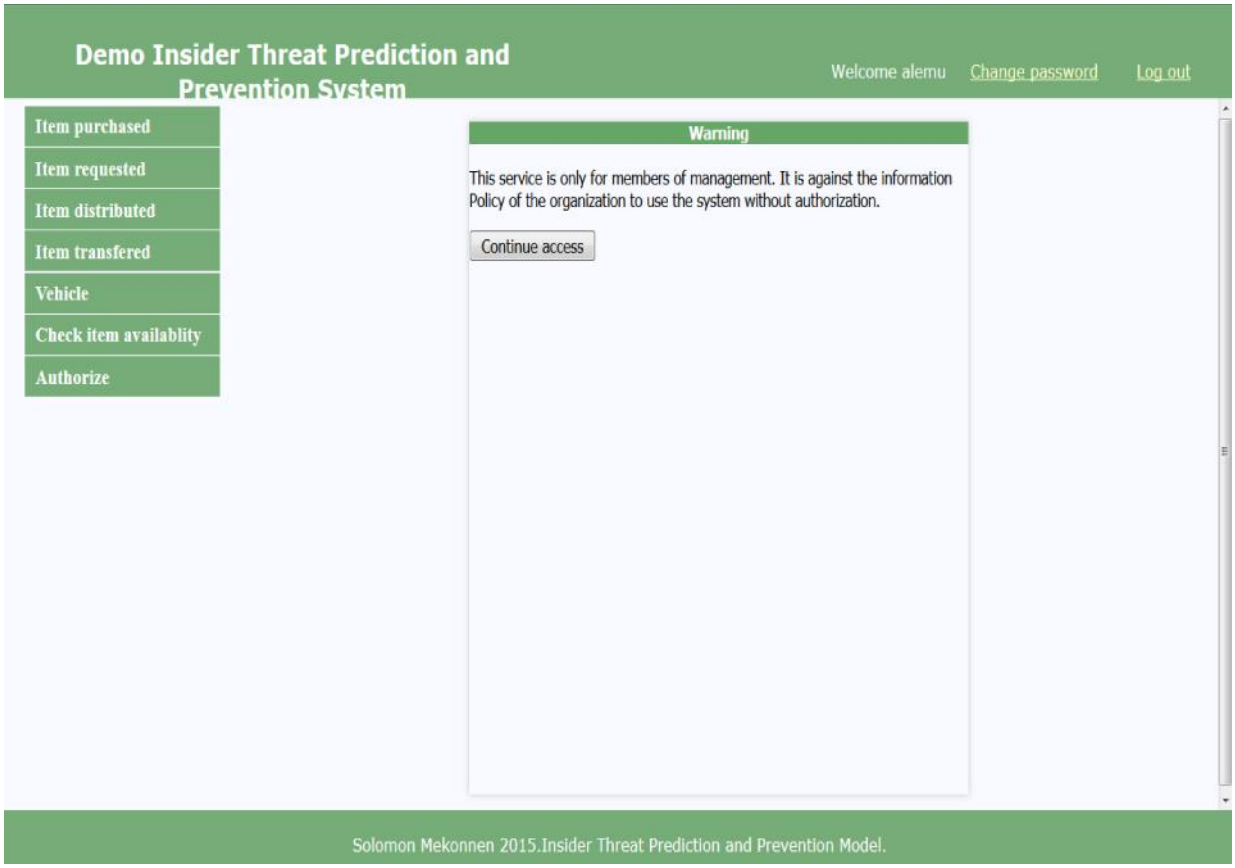

Figure 6.6 Interface: Warning to insiders

If the insiders are loyal to the organization, they are expected to not be tempted to continue access by ignoring the warning. However, if the insiders decide to continue accessing the unauthorized information, they will be allowed to access the system and authorize items which do not form part of the real system, as shown in Figure 6.7.

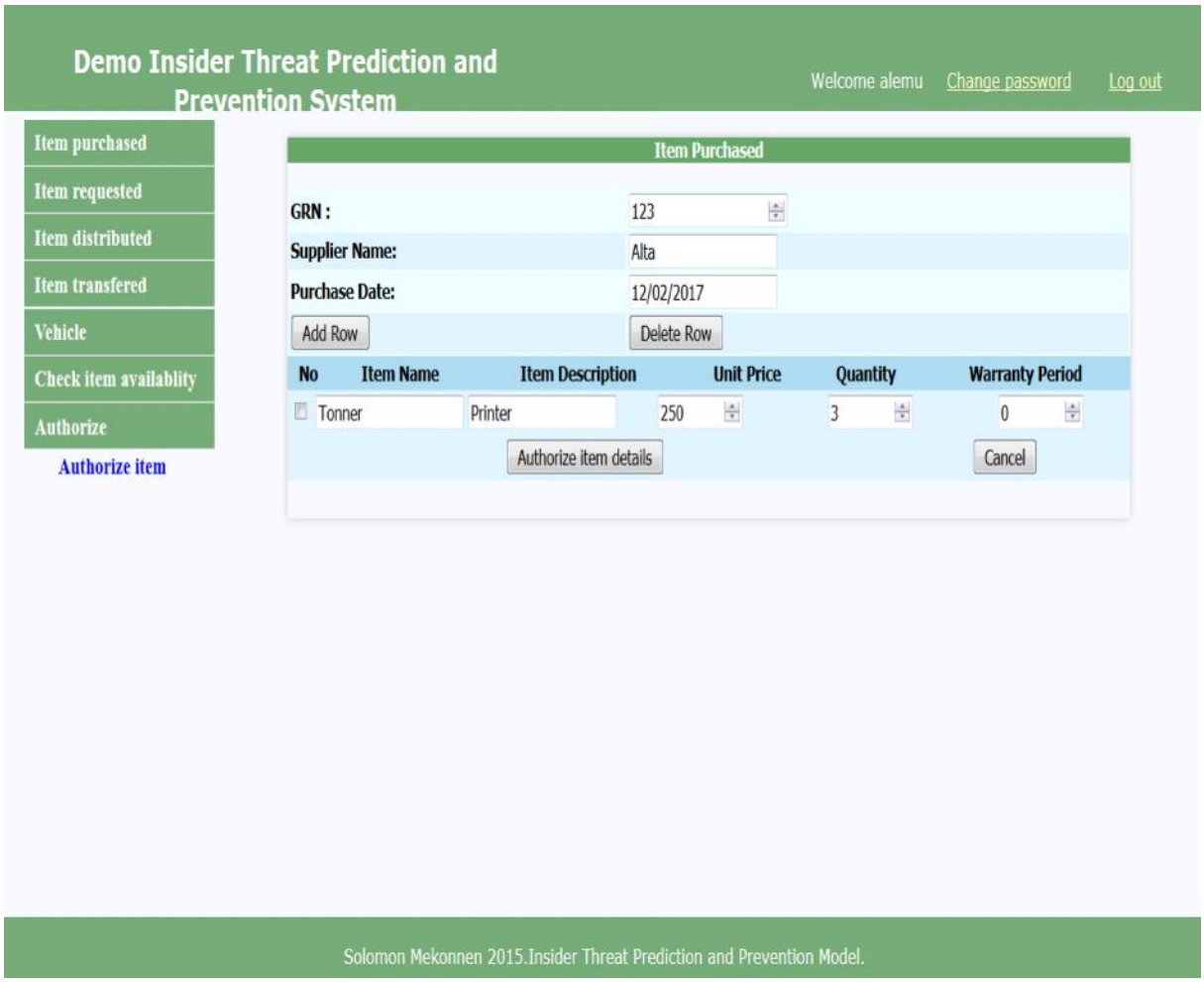

Figure 6.7 Interface: Insiders accessing the honeytoken

Once the insiders have completed the authorization of items, the prototype will provide post-neutralization mitigation which attempts to alert their conscience by determining the justification they have used to bypass the warning and access a service which falls outside of their authorized tasks. Post-neutralization mitigation is shown in Figure 6.8.

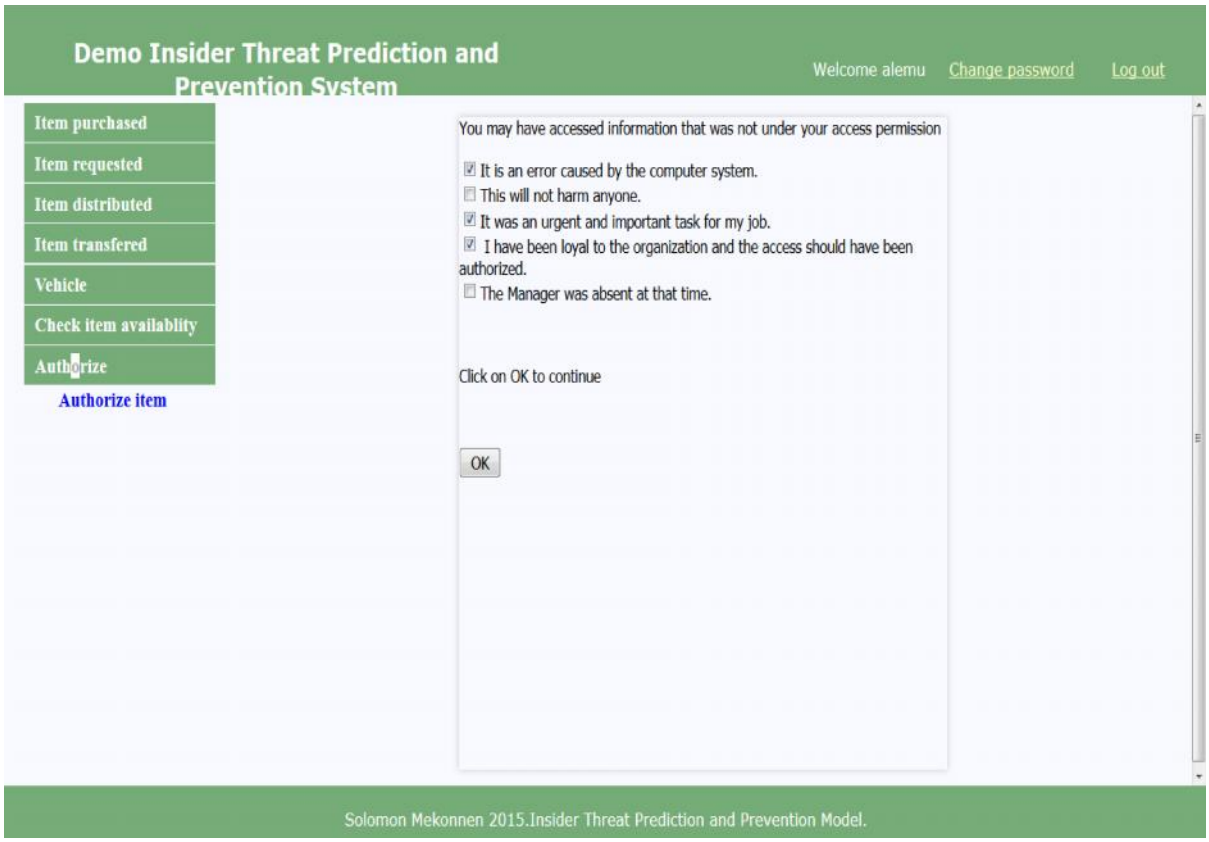

Figure 6.8 Insiders providing rationalizations

Thereafter, based on the justification the insider has provided to ignore the warning and in breaches of the IS policy of the organization, the prototype will promote the policy and assist compliance so as to educate the insider in order to deter the insider from committing future crimes. The process is shown in Figure 6.9.

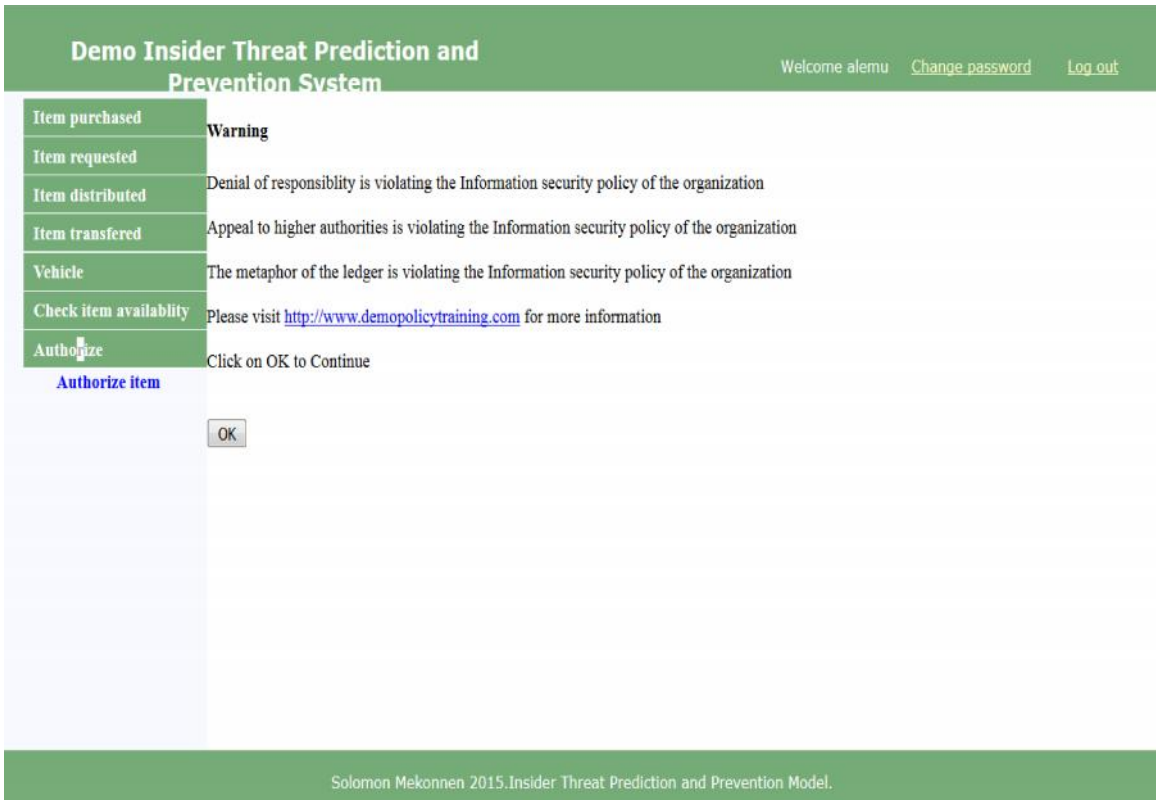

Figure 6.9 Interface: Neutralization mitigation

As is shown in Figure 6.9, the system educates the insiders on justifications provided regarding denial of responsibility, appeal to a higher authority and the metaphor of the ledger against the IS security policy of the organization, as these aspects could be used as excuses for committing the crime.

Finally, the prototype will compile and produce an anonymized report on the behaviour of the insiders so that it can be used as an input for future insider threat mitigation strategies. Opportunities and rationalizations of crime can be reduced once they are known in advance. A sample report is presented in Figure 6.10.

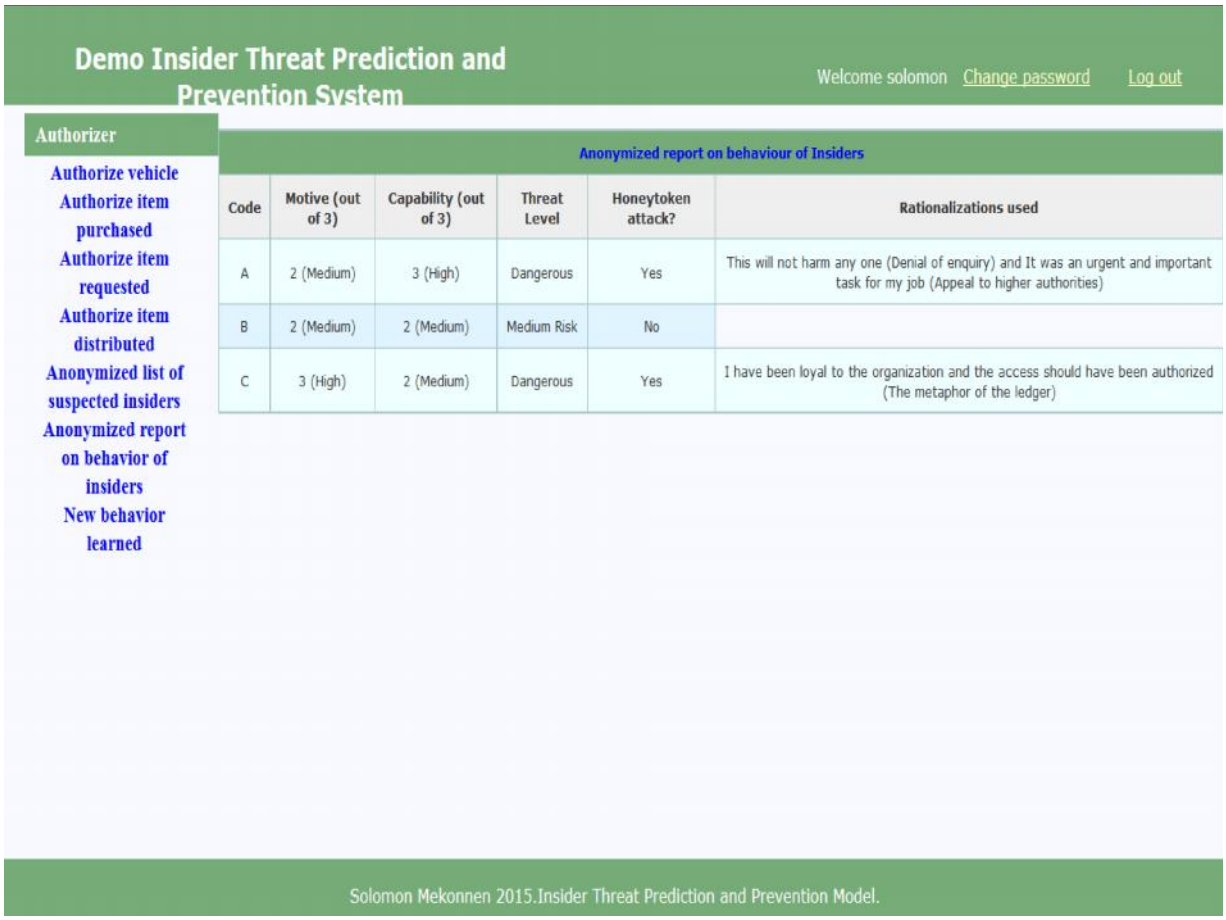

Figure 6.10 Interface: Report on the behaviour of insiders

6.2.3 Simulation

To demonstrate the model, a simulation has been produced to show how some functions of the model works in the background. A simulation for the stress recognition part of the context analyser and one for the anonymized part of the privacy-preserving filter have been produced. These simulations have not been provided to the experts for evaluation.

6.2.3.1 Stress recognition using typing pattern

One of the functions of the context analyser is to assess the current stress level of insiders by using their typing pattern to determine if there are any stressful situations that may drive them to commit a crime. According to medical studies conducted related to cognitive impairment, change in a cognitive state like high stress will affect computer interactions of individuals including keyboard stroke pattern (Jimison, Pavel, McKanna & Pavel, 2004; Jimison, Jessey, McKanna, Zitzelberger & Kaye, 2006). Research also demonstrates that when individuals experience stress, there will be a change in their typing patterns such as a decrease in typing speed, increased number of errors and the use of negative words (Khanna & Sasikumar, 2010).

This simulation records the normal typing speed of a user and assesses the current speed to determine whether the typing speed of a user is normal or not. This information will indicate the user's stress level. It also detects when the backspace and delete buttons are pressed frequently when the user makes an error. This action may be an indication of a change in the typing pattern.

For instance, if a user types 40 to 50 characters within 10 seconds, the prototype makes a record of the data and counts the number of characters until the ten seconds end. The prototype provides an output that will indicate whether the typing speed falls within the normal range of the particular user or not. For instance, as shown in Figure 6.11, the user has typed 37 words within 10 seconds which is within the range of 40 to 50 and it is normal, thus the prototype displays "The typing speed is normal".

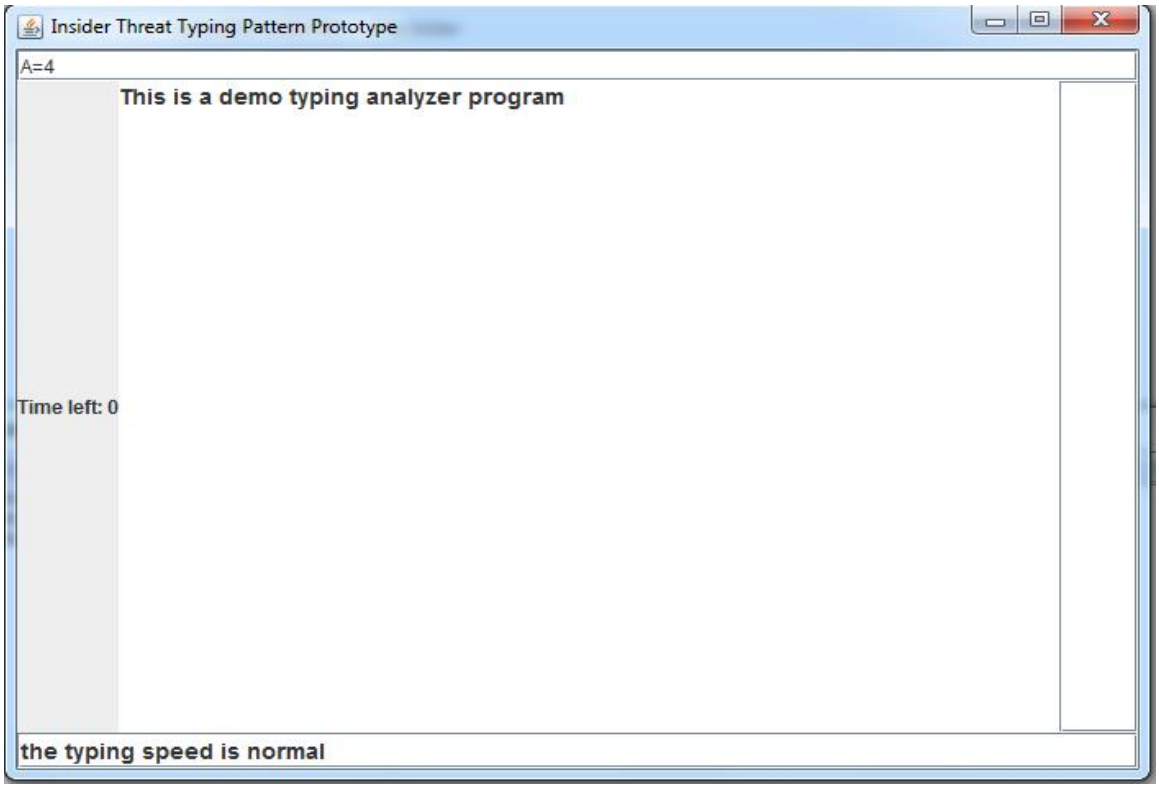

Figure 6.11 Interface: Typing pattern simulation

If a user types 21 characters within 10 seconds, it will be below the range and display "The typing speed is abnormal". This may be an indication that the user is under stress (see Figure 6.12).

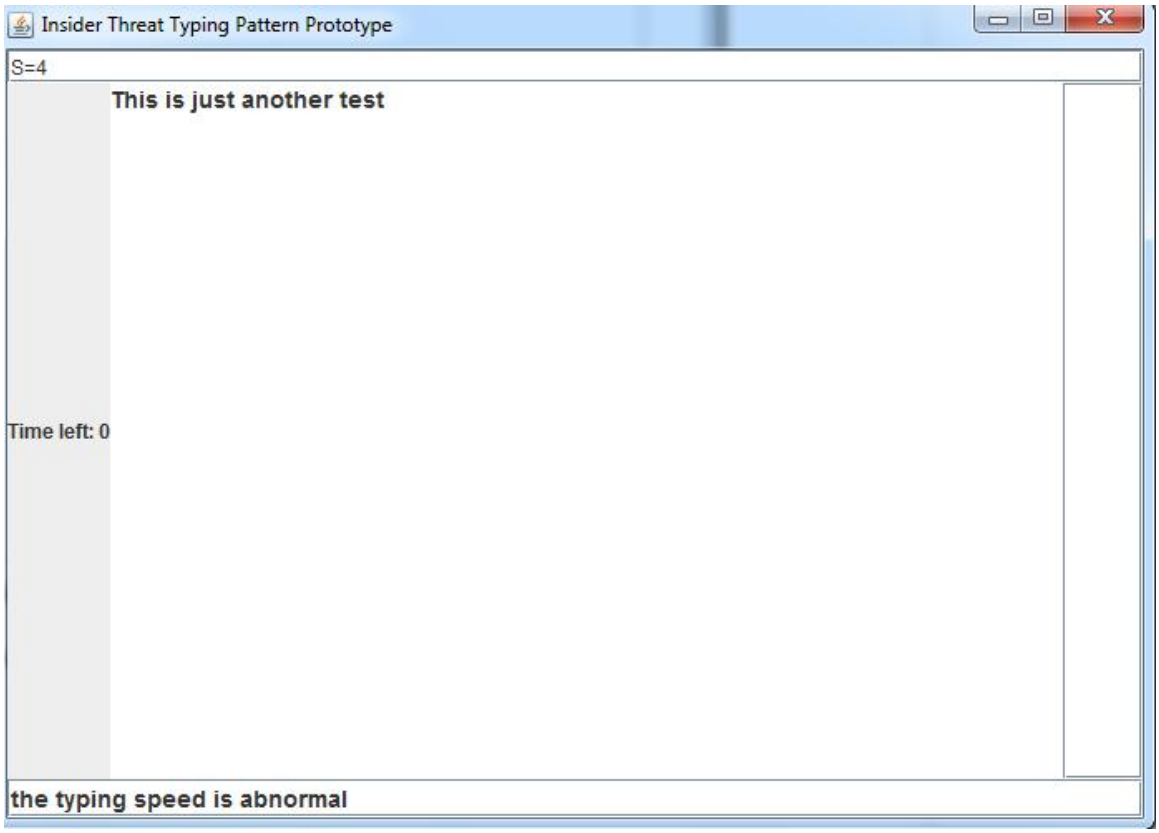

Figure 6.12 Interface: Typing pattern simulation output

The simulation can detect when a user presses the delete and backspace keys frequently when he or she has made a typing error and deletes the error, as shown in Figure 6.13.

Figure 6.13 Interface: Error sense

6.2.3.2 Anonymization

One of the techniques used to preserve the privacy of insiders is to anonymize their data so that any identifiers that might help to identify them will be removed so their privacy is preserved. For instance, Insiders' data might be described as follows:

ID AAU/125/18 Motive Medium Capability High Opportunity Yes

ID AAU/467/17 Motive High Capability Medium Opportunity No

ID AAU/5678/14 Motive Medium Capability High Opportunity Yes

From the above data it is easy for an intruder to identify the individuals, as their identification numbers are included in the data. Therefore, there is a need to anonymize this data. The simulation will take an input such as data and display an anonymized version of the data. The data is retrieved by the simulation, as shown in Figure 6.14.

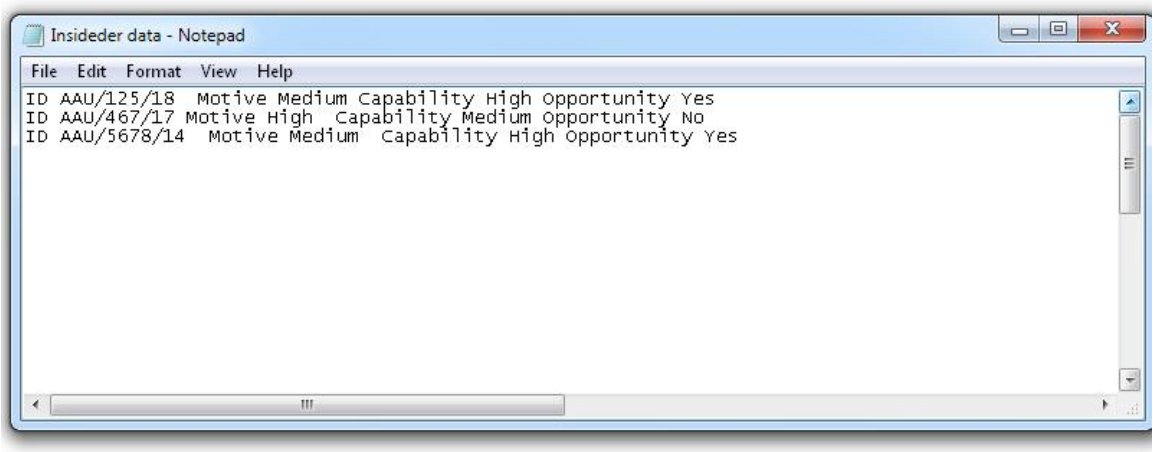

Figure 6.14 Interface: Input for anonymization simulation

As it is presented in Figure 6.14, the user will be asked to specify the location of the insider's data to be anonymized. Then the user will select any file that holds the insider's data, as shown in Figure 6.15.

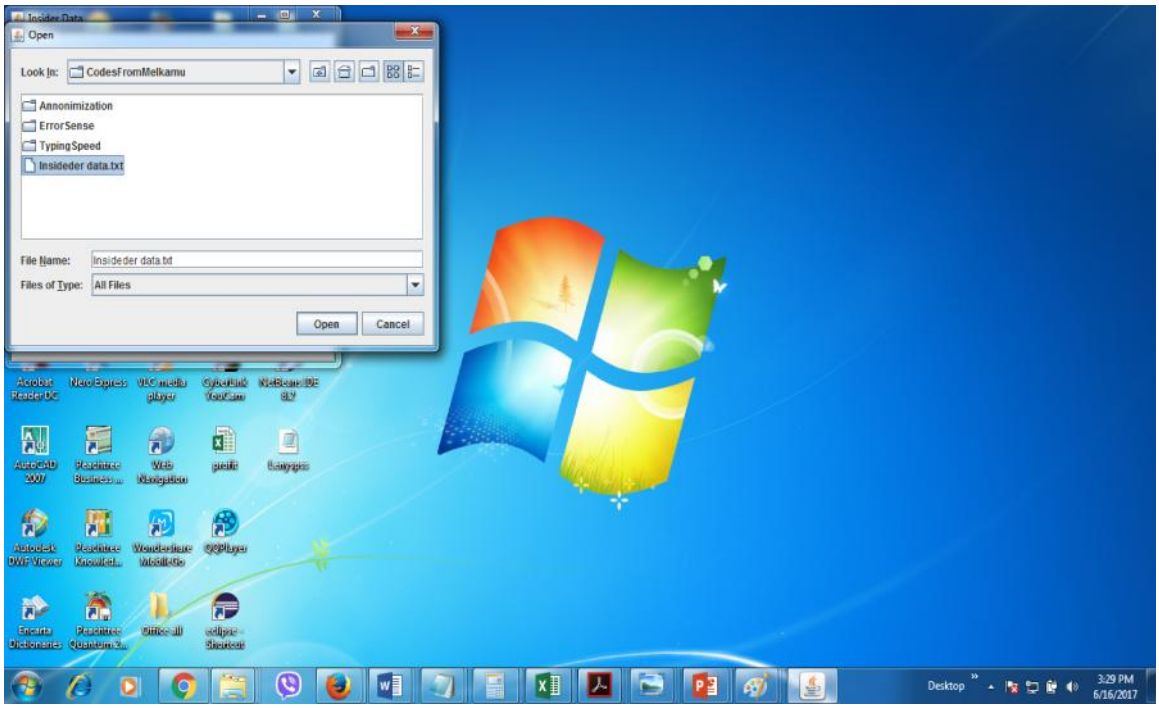

Figure 6.15 Interface: selecting input for anonymization simulation

A sample file is displayed in Figure 6.16.

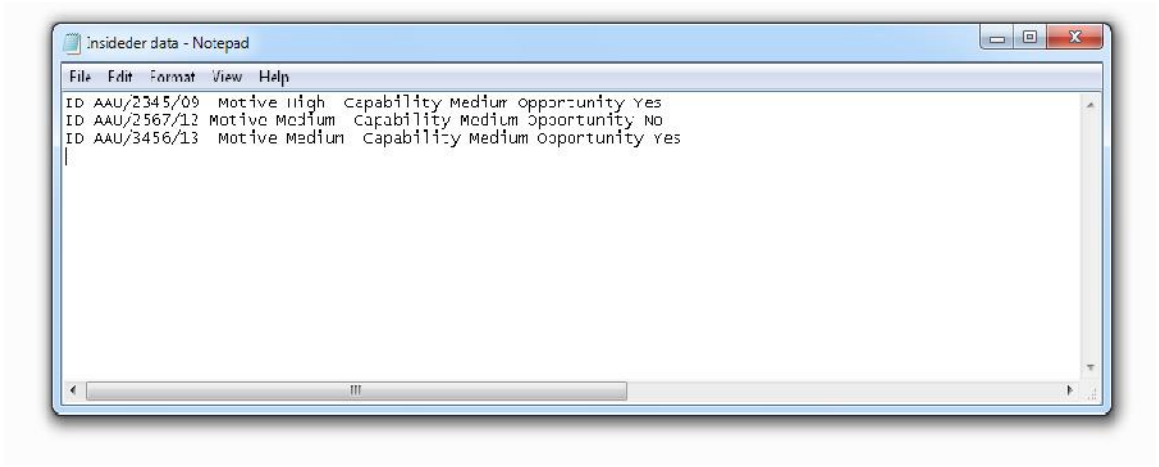

Figure 6.16 Interface: sample input for anonymization simulation

Then the simulation will take the above file as an input and display the anonymized version, as shown in Figure 6.17.

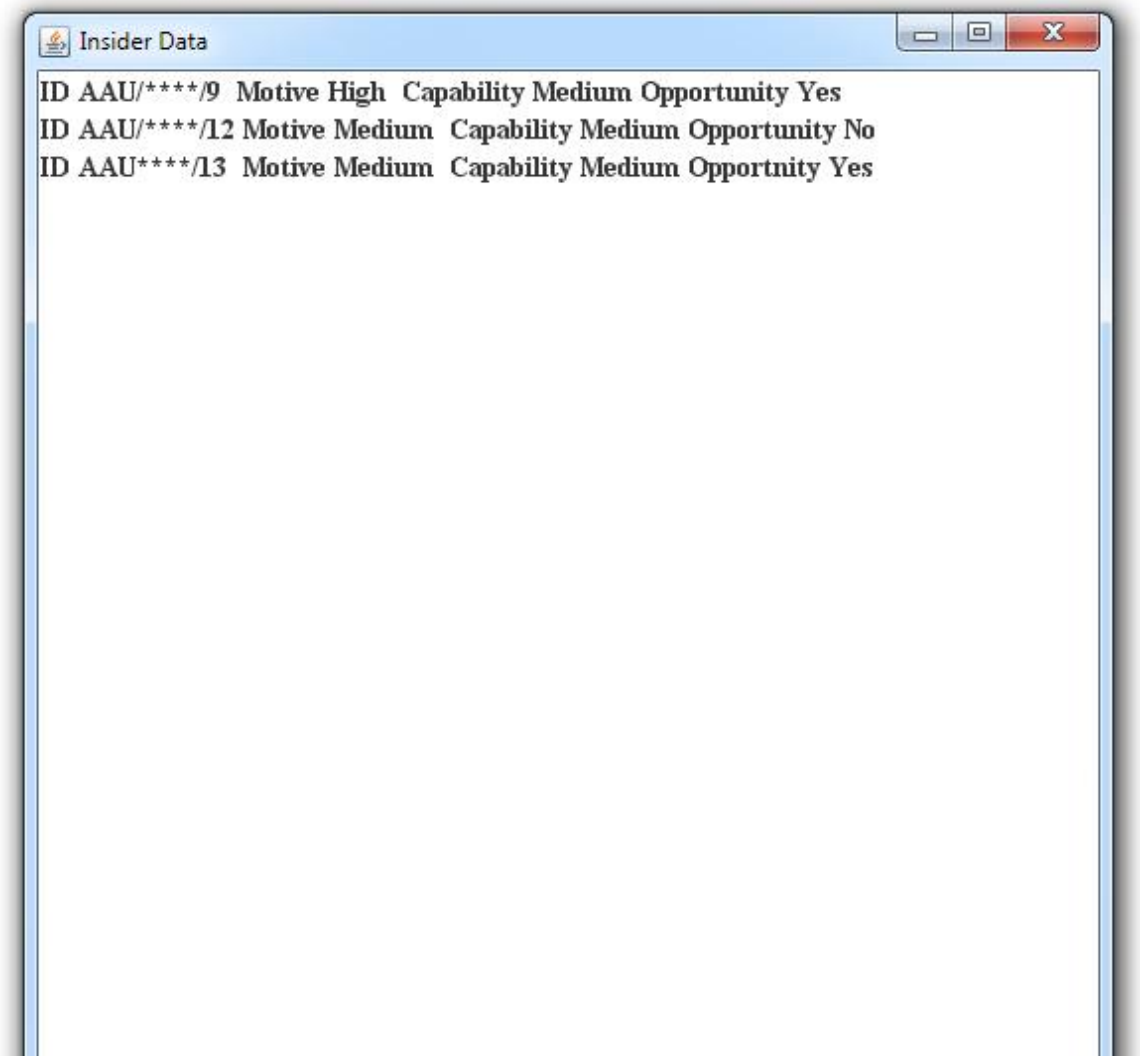

Figure 6.17 Interface: Sample output for anonymization simulation

As presented in Figure 6.17, the identification part is anonymized by replacing some of the characters by ***; for instance, ID AAU/2567/12 is changed to ID AAU/***/12 which will make it impossible to uniquely identify the individual by using his or her ID. This technique is used for the model.

6.3 Data analysis

A sample of twenty-six (26) information security experts (n=26) were selected purposively from a variety of industries to evaluate the model and prototype. The prototype contains a subset of the elements of the model. The participants completed a questionnaire designed to evaluate the model (see Appendices A and B). The response rate was 10%.

Among the participants, the highest number was information security supervisors who contributed seven participants from the total of 26 participants. The participants were categorized into six professions, as shown in Figure 6.18. There were seven information security supervisors (n=7), five information security engineers (n=5), five information security consultants (n=5), four information security analysts (n=4), two information security specialists (n=2) and three information security architects (n=3).

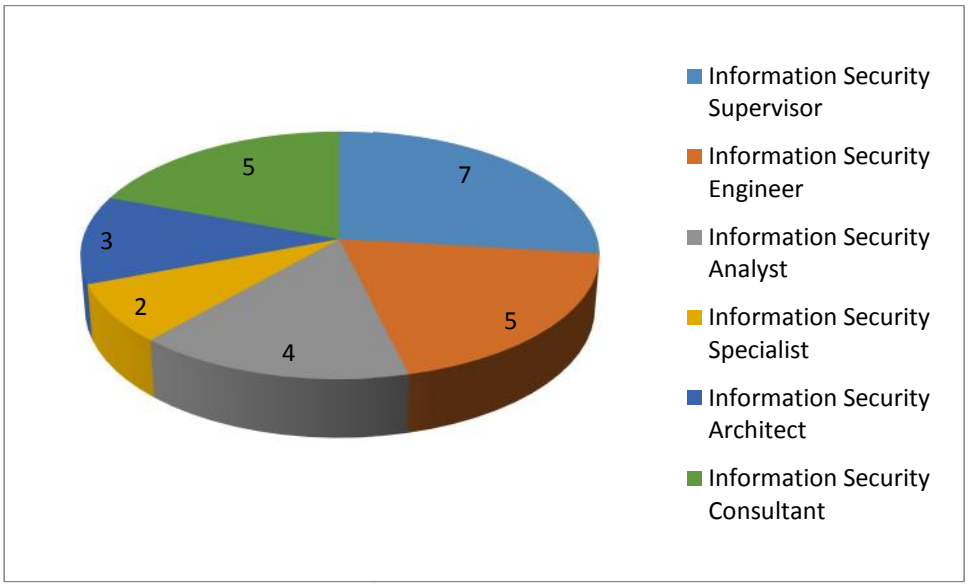

Figure 6.18 Profile of participants

6.3.1 Results of the value judgments

All factors in the value judgment ranked above 75%, relative viability ranked the highest with 94% whereas usability is the lowest with 77%, as shown in Figure 6.19.

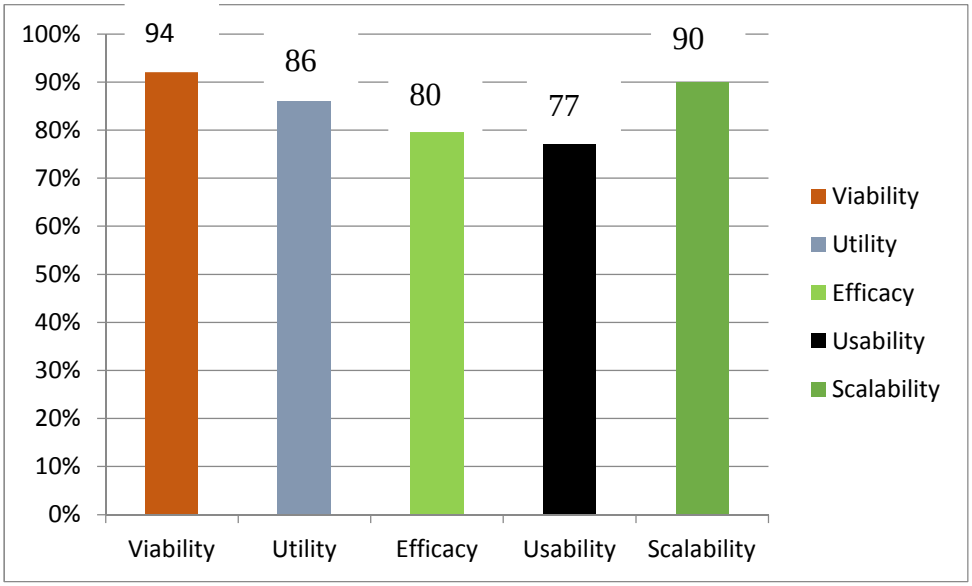

Figure 6.19 Value judgments

6.3.1.1 Viability

Overall, viability was ranked highest with a score of 94% which was based on the factors of implementability and integrability. To assess viability, Questions 1 and 5 were used.

6.3.1.1a Implementability

According to the respondents, 88% agreed that the model concept could easily be translated into an implementable product (Question 1). Some of the participants raised issues to be considered when implementing the model regarding challenges in integrating the model with other systems. For instance, Participant #13 indicated that "the time to develop plugins to major systems that you want to monitor would be quite a challenge, being that Microsoft being the easiest, however, expanding this to banking, financial sectors around the world would be the challenge". Participant #21 advised that the model

need to make sure that the data gathered by the system was not used by the management team or hackers.

6.3.1.1b Integrability

All of the participants agreed that the model could be easily integrated into the existing system (Question 5). Participants who agreed provided the following substantiations:

In support of the integrability of the model, Participant #20 remarked:

> "Currently, the ISO27001 standard on information security requires that an ISMS have continual monitoring as a requirement for its successful implementation. Therefore this model concept can be easily integrated to existing ISMS systems within organizations."

Participant #26 also provided a similar justification as Participant #20:

> "There are a lot enterprise resource systems that can interface with this model. E.g. SAP system."

Some participants expressed the view that the system might require the support from other vendors to work together. That was supported by Participant #2 and Participant #10 respectively.

> "In some cases, it may require additional development by external vendors. Will be dependent on their willingness to participate."
>
> (Participant #2)

> "As long as the interoperability is possible. In many closed/proprietary software solutions this might be an issue, but if the software organization can understand the value, they might be willing to add it as an extra feature."
>
> (Participant #10)

Participant #22 recommended that there might be a need for policy review:

> "Organizational Information and Communication (ICT) standards and policies will need to be revised with necessary approvals before implementation. E.g. password policy."

6.3.1.2 Utility

The utility of the model ranked at 86% which is dependent on the general exploitation of the model concept, the effects of the model in detection and prevention of threats, as well as the motive, opportunity and capability components, the rationalization techniques and privacy preservation. The questions that were used to derive this value will be discussed next.

6.3.1.2a Utility in terms of general exploitation of the model concept

Utility of the effects of the model in detection and prevention of insider threats

In terms of the effects of the model in the detection and prevention of threats (Question 2) 92% of the participants agreed that the model would support organizational prediction and prevention of insider threats. Some respondents who agreed also provided recommendations.

Participant #10 suggested using a human resources questionnaire as a source of detecting pressure:

> "I must admit though that you might need to include other methods of detecting if a person is under a lot of stress. Perhaps Human resource questionnaires to gauge the employee's mood and state of mind, their financial situation etc. I also need to mention that if someone is working on an IT system and is generally not a fast typer he might be suspected of being a possible threat."

The issue of learning the behaviour of insiders and making it adaptable to a specific environment was recommended by Participant #10 and Participant #26:

> "The system might need to learn, as in the case of an IDS/IPS, and in time develop profiles of users."
>
> (Participant #10)

> "The model can be customized further to meet a specific environment."
>
> (Participant #26)

Participant #12, who raised legal issues with the model, questioned the model concept:

> "Would enticing people to commit a crime not be constitute a crime in its self- [sic] in some parts of the world?"

Participant #22, who disagreed with the effectiveness of the model in the detection and prevention of insiders, criticized the model as it does not consider detection collision of accounts but focuses only on insiders working alone. The same participant argued that if the model were to classify innocent employees as insiders, those employees might be discouraged and motivated to commit a crime.

Utility of the reasonability of the model

With regard to reasonability of the model (Question 3), 77% of the respondents agreed that the assumptions in the model were reasonable. Three of the participants added some concerns to substantiate their agreement:

> "I don't think the assumptions made are unreasonable however I do not agree with the way the system measures proficiency of the users."
>
> (Participant #21)

> "I think that typing speed or incorrect login attempts need to be finely reviewed before being marked as potential threat."
>
> (Participant #16)

"Legislation on privacy is looming. Privacy is sensitive, cross-country/region even less in place. Software is more innovative than the Roman-Dutch laws. USA-EU privacy views differ, typical example, right to be forgotten etc.

(Participant #7)

Two participants, who disagreed with the reasonability of the model, provided their reservations with the keyboard stroke analyser:

"Only issue I have is keystrokes are not an accurate measure. Especially when considering English as a second, third and even fourth language."

(Participant #11)

"I certainly agree that the keystroke analysis tool might not always reflect the true reflection of a change in a person's behaviour. I believe that mistakes might also be caused by the level of concentration at the time of typing, which does not always reflect stress levels. However, the overall concept is not far-fetched."

(Participant #20)

Utility of the benefit of the model for decision-making

With regard to the benefit of the model for decision-making (Question 4), 96% of the participants agreed that the proposed model could be used as a framework to aid organizations in information systems security investment or the development of decision-making processes to address the insider threat problem.

One of the participants (Participant #7) who agreed suggested that "the model should consider the implementation of expanded new generic top-level domains that means there might be many uniform resource locators ending .club, .xyz and .guru". He added that "For now, they are primarily an asset being cultivated by criminals to confuse users and to ensnare and entrap their computers with malware."

From the respondents who disagreed, Participant #19 asserted:

> "I cannot see how the proposed model can benefit firms in information security investment. However, I think it can benefit firms in driving compliant user behaviour [sic]".

6.3.1.2b Utility related with motive component

Utility of the keyboard stroke analyser

In terms of the keyboard stroke analyser (Question 9), 77% of the participants agreed that the emotional state of insiders (i.e. stress levels) could be predicted, based on their keyboard strokes information, such as changes in typing speed, duration of a keystroke and the rate of mistakes.

Some of the respondents, who agreed on the effectiveness of the keyboard stroke analyser, provided feedback on the implementation, including considering different scenarios of employees, learning the normal typing behaviour of employees and managing false positives.

> "Only if the employee is genuinely not clumsy on the keyboard or no physical impairment occurs during the sampling period."

(Participant #2)

> "I agree only if you had a baseline of employees 'normal' behaviour, which can be compared to deviance."

(Participant #12)

> "Agreed. However, such prediction needs to cater for false-positives as a result of inadvertent actions."

(Participant #18)

Those participants who disagreed with the effectiveness of the keyboard stroke analyser raised different issues, including its dependence on whether the fluency of employees in the language they use and their passion for work activities.

> "Do not agree with this. Keystrokes are not an accurate measure, especially when considering English as a second, third and even fourth language."
>
> (Participant #11)

> "My typing speed changes naturally depending on my passion of case I am working on."
>
> (Participant #16)

Participant #13 commented that the keystroke analyser might have false positives, stating that "… keystrokes are good however as an example of a false positive, a new school leaver gets a job as a PA (personal assistant) to the executive team, first few weeks on the job [sic] nervous, your system would flag her, thus the method is good but has flaws."

Participant #23 argued that there were some professionals like coder types whose typing speed could not be affected by stress.

> "For example, coder types will have very high keystroke rate with the minimal error based on their level of comfort with finger-to-keyboard and confidence – doubt this would change significantly when 'under stress' ".
>
> Participant #13)

Utility of the resource usage analyser

With regard to the resource usage analyser (Question 10), 81% of the participants agreed that change in resource usage behaviour (like search behaviour and download behaviour) is a viable indicator of malicious intentions. Participants who agreed with the effectiveness of the resource usage analyser offered the following caveats:

> "I agree but would need advanced analytics to be accurate."
>
> (Participant #16)

> "Completely valid. Suggest also that centralized logging of user activity together with user behaviour profiling are your most accurate indicators of potential for (or actual) malicious acts."
>
> (Participant #23)

> "I used to manage a proxy server for a government department. I once picked up a user who is downloading invasive software. The Intrusion prevention system (IPS) later that day detected a port scanner from inside the Local area network (LAN) which was easy to track back to the user. The user was performing a scan on the production environment for his assignment. Even though the intentions were good, the scanner saved the log which contain important information about the organization systems."
>
> (Participant #26)

Some participants who agreed also added suggestions for improvement:

> "Typically, environments differ but policy should be there to protect the use of organization-wide resources. Breach would invoke disciplinary action."
>
> (Participant #7)

> "Again suitable baseline is in place. Source and destination should be well investigated, and blocked if need be."
>
> (Participant #12)

> "In addition to that, we could include other indicators such as surfing of malicious websites, installation of offensive software, and other surfing patterns that could reveal variations in insiders' lifestyle."
>
> (Participant #18)

Some respondents who disagreed provided the following substantiations:

> "All indicators of a person might not be seen electronically, some might be physical however it's a good place where you are at."
>
> (Participants #13)

> "I do not fully agree with that due to the fact that in my experience, employees more often abuse resources simply because there is an opportunity to do so."
>
> (Participant #20)

> "It will only be an indicator for a low-level environment where there are lots of repetition as part of the work."
>
> (Participant #25)

6.3.1.2c Utility related with opportunity component

Utility of the effects of understanding opportunity in minimizing cybercrime

In terms of the benefit of understanding opportunities in minimizing crime (Question 11), all of the participants agreed that understanding the opportunities (e.g. weak access controls) that an insider might use to launch an attack will help in minimizing the risk of cybercrime.

Three participants who agreed also provided the following additional justification for their agreement:

> "Without opportunity, crime could not be perpetrated."
>
> (Participant #11)

> "Cybercrimes committed by insiders are largely triggered by opportunity rather than the target (crime of opportunity vs. crime of target)."

(Participant #18)

> "100%. If you have controls in place around segregation of duties (e.g. Ensure development resources have minimal access to production systems.), No usage of System Accounts from console etc. are good mitigations."

(Participant #23)

Participant #10 suggested that the user's level of expertise would also need to play a part in this method of identification.

Utility of the level of the access analyser

With respect to the utility level of the access analyser (Question 13), 88% of the participants agreed that the level of access (i.e. systems role) granted to an insider (i.e. administrator, advanced user, novice) could be a means of identifying insiders who might be future threats to an organization's IT infrastructure.

Some respondents who agreed provided the following justifications for their views:

> "Well balanced controls and education for all will protect organization-wide assets. Essentially, administrators need to be audited annually. Annual audits need to become the norm, nature of the business to see if controls are effective."

(Participant #7)

> "That is why there should be privileged user monitoring, centralized logging etc. for highly privileged users but as stated elsewhere we need these resources in IT, likely more than any other. But this better based on actual levels of access than just level of proficiency."

(Participant #23)

Participant #10 who also agreed recommended that "keep track of this kind of user's social media interaction like what sort of pages do they like, the posts they put up on their wall etc."

Two participants who disagreed provided the following substantiations for their disagreement:

> "I disagree. The level of access could increase or decrease opportunity. But it cannot be used to identify insiders."
>
> (Participant #5)

> "The test is too linear and needs more variables."
>
> (Participant #16)

6.3.1.2d Utility related to the capability component

Utility of the capability of a user in using information systems

In terms of the capability of a user in using information systems (Question 14), 96% of the participants agreed that the capability of a user in using the information systems of the organization (i.e. user sophistication) could be a factor for insider threat mitigation, as users need to be capable of exploiting the organization's IT infrastructure in order to commit a cybercrime.

Two participants who agreed added the following caveats:

> "In real life, the capability is often the factor which makes the difference between being caught or getting away with the perpetrated fraud."
>
> (Participant #2)

> "That is why there should be more controls around privileged accounts and users, like logging etc. Disagree, however, that this is based on individual capabilities though. Actual privileges [sic] available to the user i.e. can create, retrieve, update

and delete (CRUD) rights on the database or backend of the transactional system is a much more reliable indicator of risk than 'wow this guy programs in C#!' "

(Participant #23)

One of the participants who differed provided the following reasons for the disagreement:

"Committing cybercrime has become easier to achieve due to the readily available tools that do not require sophisticated Information Technology (IT) skills to launch an attack. One other factor that should be considered is the negligence loss of data. Attacks/data loss do not all require intention as an element, a mere negligence by an internal employee may pose a threat to the confidentiality or integrity of the organization's data."

(Participant #20)

Utility of the error and warning message analyser

With regard to the utility of the error and warning message analyser (Question 15), 81% of the participants agreed that the number of errors and warning messages generated by the user while using an organization's IT infrastructure could be one of the indicators to assess the skill levels of the relevant user.

One of the participants (Participant #16) who agreed asserted that:

"Agree but not always - needs more variables like amount of errors and frequency in short period of time".

Two participants who disagreed provided the following substantiations:

"Depends on the technical control. Data loss prevention (DLP) will generate a lot of warnings etc. before sending a mail with sensitive info. Also, what about different software versions? Going from word 5.1 to word 10 will cause me to make a lot of errors, but it does not mean that I am not skilled. What about moving from Outlook to GroupWise? I still receive a lot of errors on GroupWise

due to me not being familiar with the product, but that is not to say I am not a very good Exchange administrator or mail user." Participant #5)

"Experience has taught me that is only achievable in a perfect IT environment where there is no downtime and systems do not crash at will. Therefore it's a good start but provisions should be given for errors which are the system's fault rather than the human."

(Participant #20)

Utility of user profiling to determine the sophistication level

In terms of the utility of user profiling to determine the sophistication level (Question 16), 85% of the participants agreed that user profiling to determine the sophistication level (i.e. capability) of insiders could be achieved by means of an examination to evaluate the knowledge of insiders with respect to computer usage (in terms of operating systems in use, techniques implemented, familiarization with specific technologies, etc.).

Some respondents who agreed also provided the following suggestions for improvement:

"I also think that tracking the training they attend or show interest in, the books (manuals) they read, the certification/s and accreditation they achieved could all form part of this method of profiling."

(Participant #10)

"A skills gap assessment survey could also come in handy."

(Participant #18)

"Typically normal users do not have privileged access and it is limited to a need to have a basis."

(Participant #25)

Participant #5 who agreed also mentioned his concern that the component will place a huge administrative burden on companies or the recruitment process. Two other participants who also agreed provided the following comments:

> "Limited. One's circumstances can change behaviour. Consistency determines one's behaviour."
>
> (Participant #7)

> "There could be a behavioural component here such as context-aware authorization that could also be brought in. For example here is a 'bank teller' is logging in or transacting on the system after the branch is shut – Deny and Report."
>
> (Participant #23)

Utility of the insider capability analyser

With regard to the utility of the insider capability analyser (Question 17), 92% of the participants agreed that the capability of insiders could be verified, based on the types of applications they use and the level of computational resource usage consumed.

Two of the participants who agreed also provided some suggestions:

> "It should include determinant like systems knowledge, sub-systems written, interfaces, exits coded access in supervisor key etc."
>
> (Participant #6)

> "Agree 100% and I would also suggest you focus the 'skill' side of your opportunity/motivation factors on actual user privileges assigned rather than something like 'this guy a.Net wiz'."

(Participant #23)

From those participants who disagreed, Participant #22 remarked that:

> "Organizations usually have a list of applications approved for usage in that particular organization. It is therefore possible that all applications available to all users are easy to use".

Participant #16 disagreed with justifying that there are many other factors which are not considered but still have an influence.

6.3.1.2e Utility related to the rationalization component

The utility of rationalization techniques

In terms of the utility of rationalization techniques (Question 18), 85% of the participants agreed that understanding the rationalization techniques which insiders might use to justify their crime could be used to design a neutralization mitigation strategy to circumvent any excuse for committing a crime in future.

The utility of situational crime prevention techniques

With regard to the utility of situational crime prevention techniques, 81% of the participants agreed that posting instructions (e.g. e-mail disclaimers) could be used to remove excuses for a crime. Regarding the mitigation of the insider risk (Question 19), 96% of respondents agreed that alerting conscience (e.g. via a code of ethics) could be used to remove excuses for a crime and mitigate the insider risk (Question 20) while 88% of the participants agreed that assisting compliance (e.g. hacker challenges) could be used to remove excuses for a crime and mitigate the insider risk (Question 21).

Participant #21 remarked that awareness campaigns in connection with IT policy and the consequences of breach thereof were likely the best deterrents.

Utility of setting rules

With respect to the utility of setting rules (Question 22), 96% of the participants agreed that setting rules (i.e. policy) which explicitly invalidated any potential defences (i.e. excuses) for cybercrime might be a useful mitigation strategy. This implies resetting the rules should be based on new justifications for cybercrimes.

6.3.1.2f Utility related to privacy preservation and the context analyser

Utility of privacy preservation

In terms of the utility of privacy preservation (Question 24), 73% of the participants agreed that collecting metadata only, such as search behaviour, file access, keystrokes and linguistic features without collecting the content of employees' communication could help to balance privacy issues associated with insider threat detection.

Utility of the context analyser

With regard to the utility of the context analyser (Question 26), 81% of the respondents agreed that understanding the context of an insider by considering the elements of usage behaviour, stress levels, and the rate of error and warning messages generated is a useful mechanism towards mitigating the insider threat.

Some participants who agreed also provided the following suggestions:

> "Careful on the system errors, i.e. poorly trained, or pushing the boundary in applying something new on the job. Consider the obvious, people who just got

warnings, be wary of social reports of user excessive level of gambling, someone missing out on promotion etc." (Participant #11)

"Could be. Would rather test the theory in practice." (Participant #24)

Participant #7 who disagreed on the utility of the context analyser commented that "stress could be a personal[sic] i.e. loss of a loved one".

6.3.1.3 Efficacy

The efficacy of the model was ranked at 80%, which was based on the efficacy of the detection of pressure, honeytokens, and anonymization.

6.3.1.3a Efficacy of detection of pressure

With respect to the efficacy of detecting pressure (Question 8), 81% of the participants agreed that detection of pressure (e.g. anger, frustration or despair due to organizational factors such as denial of salary increases or personal problems that would motivate insiders to commit maleficence) is an effective means of insider threat mitigation.

Participant #7 who agreed remarked as follows: "This is identified as one of the common issues from case studies."

Two participants who agreed offered the following suggestions:

"While detection of pressure is an effective means of insider threat detection, it may become less effective if the pressure detection program does not learn new behaviour."

(Participant #18)

"However it may be difficult to reliable source 'flags' around personal problems. Denied increases or promotions should be easily obtained from Human Capital area. Question is would they not view this as a breach of confidentiality. Have

you considered sourcing financial pressure from Credit Bureau etc.? This is often more reliable."

(Participant #23)

Participant #12 who disagreed raised the following question: "Maybe, but what about people who have infiltrated the business with the number one objective of stealing?"

6.3.1.3b Efficacy of honeytokens

In terms of the efficacy of honeytokens (Question 12), 77% of the participants agreed that deploying honeytokens (i.e. deception traps to lure insiders) by means of extraneous links, fake information on a database and so on is an effective technique to identify future threats.

Some participants who agreed added the following suggestions:

"As long as it's not done by some form of entrapment. Many users are generally curious and this should also be taken into consideration to ensure that you don't turn honest users into perceived criminals."

(Participant #10)

"I would check the legal angle here, especially in some parts of the world."

(Participant #12)

"I really like this aspect, you could use other means via this solution to understand a person more on personal elements which helps build a deeper profile."

(Participant #13)

"Honeytokens is a great start. I suggest you also include darknets and honeypots for insiders with elevated capabilities."

(Participant #18)

> "However I disagree that tripping honeypots/honeynets should be decontextualized. Why protect the privacy of someone already quite clearly up to no good?"
>
> (Participant #23)

Some participants who disagreed gave the following substantiations:

> "The Federal Bureau of Investigation (FBI) uses it to setup - Fabrication bureau of investigation. Get yourself and your organization in trouble. Carly Florina who was the Chief executive officer (CEO) of Hewlett-Packard was fired because she breached USA constitution. Need a court order ... etc."
>
> (Participant #7)

> "Not always - I would happily test a system's safety in my organization even if against policy but would report it as soon as any vulnerability is found."
>
> (Participant #16)

6.3.1.3c Efficacy of anonymization

With regard to the efficacy of anonymization (Question 25), 88% of the participants agreed that anonymization (i.e. removing identifiers) is an effective technique to protect individuals' identity when releasing sensitive information about potential insider threats.

6.3.1.4 Usability

In terms of usability (Question 23), 77% of the participants agreed that insider threat prevention and detection strategies should not infringe upon the privacy of insiders.

Some of the participants who disagreed justified that employees should not expect 100% privacy in the work environment. This has been exemplified by a participant who remarked that "the workplace is generally not a private place and employees are hired for the purpose of attending to the employers' business, not personal matters."

6.3.1.5 Scalability

The scalability of the model was ranked at 90% which depended on the practicality, applicability and the model concept.

6.3.1.6 Practicality

With regard to practicality (Question 6), 84% of the participants agreed that the model would be scalable in a real-world context.

Participants who agreed provided the following suggestions:

> "As long as the interoperability is possible."
>
> (Participant #10)"

> "I think it could be applied in higher risk environments and not necessarily everywhere."
>
> (Participant #11)

> "Really depends on the case in hand. Some applications do not have Application programming interfaces (API's)."
>
> (Participant #16)

Participant #8 who disagreed commented that "the model does not address the complexities that exist in large corporate".

6.3.1.7 Applicability

With respect to applicability (Question 7), 96% of the participants disagreed that there were no conceivable environments in which this product concept would be applicable.

6.3.2 Validation

According to Österle et al. (2011), validation needs to be checked for IS research using the design science methodology in terms of four principles which are abstraction, originality, justification and the benefit dimensions of the model concept.

6.3.2.1 Abstraction

With regard to abstraction (Question 2.1), 65% of the participants agreed that the model could solve the insider threat problem.

The participants who agreed provided the following justifications for their views:

> "Yes, it does however need to have different metrics for different groups. Employees from different classes are affected by different triggers and they respond differently."
>
> (Participant #1)

> "Yes it does as it has shown a better analysis of what usually happens within organizations."
>
> (Participant #4)

> "The model concept will surely curb the issue of insider threat problem; the solution has highly addressed the four elements of fraud and its solution."
>
> (Participant #9)

> "Yes - it is complex, and there may be some legal points to consider."
>
> (Participant #12)

> "Yes it does - impressed with the model."
>
> (Participant #19)

> "Yes, this model does help continually monitor insider threats activities and the potential of one occurring. Given the proliferation of the use of computer devices

in most organizations, this model will be applicable to many with just an exception of those who still use hard copy filing systems and no systems."

(Participant #20)

"Yes, it is a good way to assess levels of risk. As stated elsewhere though I would rely more on the organizations sources for information on powerful accounts and privileged users than more ethereal 'skills tests'. Would expand on Honeytoken side with multiple trip wires around gathering user privileges in violation of Separation of duties (SOD), abnormal behaviour in logs like deleting entries etc. I am guessing [sic] most IT savvy guys would smell a rat if you pushed them a link though."

(Participant #23)

"The concept is well informed and based on fraud prevention and information security principles and best practices."

(Participant #24)

Twenty-seven percent (27%) of the participants agreed that the model could partially solve the insider threat problem.

Those participants gave the following substantiations for their views:

"To a certain extent as it is not a 360-degree coverage ..."

(Participant #8)

"In part yes, it would be useful as part of a broader cyber defence programme."

(Participant #15)

"It is a good idea but needs more variables and stronger formula to become more accurate."

(Participant #16)

> "It helps to eliminate some aspects of insider threats, however, I [sic] feel it most threats remains and other techniques like continuous compliance training are required to educate the users about insider threats and their consequences."
>
> (Participant #21)

> "It could be, but a practical solution via a proof of concept would be superior."
>
> (Participant #25)

The remaining 8% disagreed that the model did not solve the insider threat problem. These participants argued that the insider threat domain was dynamic and it required the solutions to evolve with the changes in the environment, as intruders exploits loopholes to commit a crime. The participants provided the following reflections for their disagreement:

> "I don't think any model would be able to solve the insider threat problem. As long as there are ways to circumvent a security tool, people will try to exploit it. This is where organization policies would come into play as it would state that regardless of the person's intent, the consequences remain the same. This might seem harsh, but it will mean that employees think before they act, as they know that actions will have consequences."
>
> (Participant #10)

> "No, it attempts but does not solve, as the insider threats are always changing with the times. It is more of a people issue."
>
> (Participant #14)

6.3.2.2 Originality

With regard to originality (Question 2.2), all of the participants except two agreed that the model was original.

Those participants who agreed provided the following comments:

> "Yes. The insider threat requires real-world solutions. Next step is to actually implement these models in a real-world scenario."
>
> (Participant #2)

> "Definitely. I also think that this sort of model needs to be built into the OS, which will effectively provide for interoperability with all the applications on the system. We are losing the battle in the efforts to stem cybercrime, and the biggest problem is the fact that there are no real means of establishing a proper profile of the perpetrators - i.e. there is no ONE thing linking these people or that they have in common."
>
> (Participant #10)

> "Yes, I think this is a great step towards dealing with a threat that will always be present."
>
> (Participant #11)

> "Yes, I think this is a great concept that has great potential for information security."
>
> (Participant #13)

> "Yes, the psychological and criminology aspects add another layer."
>
> (Participant #15)

> "Yes, this model is more focused on detection and analysis of the potential threat. It could be adjusted a little too also include the element of awareness by fostering a behaviour of informing employees of their information security responsibilities as they navigate and perform certain activities on the application."
>
> (Participant # 20)

> "Yes, the model combines factors that help shed light on different dimensions to I insider threat. The model further offers perception that isn't otherwise obvious to information security e.g. stress levels and the combination of errors committed."
>
> (Participant #22)

> "It is definitely an original stance in terms of risk profiling the organization's risk exposure."
>
> (Participant #24)

> "Potentially yes if it works in practice. The points of departures make sense in theory, with the understanding that it will not be fool proof. Have to consider the practical implications of real systems as well."
>
> (Participant #25)

The two participants who were not sure the model was original gave the following comments:

> "Yes and no. Security information and event management (SIEM) do this to some degree. But I haven't seen any SIEM systems that go to this level on insider threats."
>
> (Participant #16)

> "Need to check out solutions from organizations like CERT (division of the Software Engineering Institute)."
>
> (Participant #7)

6.3.2.3 Justification

In terms of justification (Question 2.3), all of the participants except one agreed that the model was justified.

Some participants who agreed also provided the following caveats:

> "Yes, it is justified but more could be added as criminals are always ahead and research should always continue to discover new threats."
>
> (Participant #4)

> "Yes. I do understand the concept."
>
> (Participant #8)

> "Yes. Agreed. Well understood."
>
> (Participant #14)

> "Yes, the model has taken all the key elements to potential insider threats into consideration.
>
> (Participant #22)

> "Yes it does and many organizations would benefit from it."
>
> (Participant #24)

Participant #15 who disagreed forwarded his reservation on the detection part of the model, stating: "There could be a little more detail around how exactly the model flags users and what the implications are thereof, as well as next steps to add a little more context to the model."

6.3.2.4 Benefit

With regard to benefit (Question 2.4), all participants except two responded positively to the benefit aspect of the model concept.

Those participants who agreed that the benefit would be realized in the future but not immediately provided the following substantiations:

"Future. Need to implement, across the strategy platform. All new implementations need to address security compliance issues."

(Participant #7)

"I believe in the future as we are changing again to cloud-based systems so you in the middle and right now many are in limbo."

(Participant #13)

"The benefits will not be realized immediately, but it will benefit in a long run."

(Participant #18)

"The benefit will not be immediate, just like any newly introduced systems, people will need to first get used to it and start exploring. Therefore, results will start yielding after a while."

(Participant #20)

"Likely that it could be valuable in future, you may want to look into making your prototype more of a 'framework' than an application. That way various organizations and their IT Security departments can configure inputs to the opportunity, motivation, and factors."

(Participant #23)

Some participants who agreed on the benefits provided the following comments:

"Yes, this contributes towards research conducted in this field."

(Participant #2)

"To a certain extent as it improves off the shelf solutions available with several limitations."

(Participant #8)

"If the profiling mechanisms get enhanced and the interoperability exists then this would be of an immediate benefit."

(Participant #10)

"I think so - integration into other systems would be +++."

(Participant #12)

"Yes, but It depends on the security maturation of the organization ... In South Africa, we are probably a few years away from adopting a model like this."

(Participant #15)

"Yes, firstly organizations can formulate policies that will not hinder their ability to mitigate insider threats. Secondly, organizations and industry can improve their best practices when evaluating their information security strategy."

(Participant #22)

Participant #14 who was not sure of the benefit responded that "no idea, until tried practically and evidence adduced".

Participant #24 who did not agree remarked, "Insider threat is still a not yet very well understood concept by many organizations and this bridges a gap currently and in future in Identity and User Management as well a fraud prevention and information security."

6.3.3 Recommendations

Some of the recommendations provided by the respondents related to caution that should be taken on implementing the model are the following:

"I believe that further consideration should be given to legal disclaimers users acknowledge on a sign on."

(Participant #5)

> "Caution legal entrapment in some countries."

(Participant #12)

Some of the respondents recommended that there should be a due consideration in implementing and integrating the model into real-world environments:

> "Would have liked to see a practical implementation (real-world scenario)."

(Participant #2)

> "You will need to factor in people, process, and technology involvement during the implementation of such a solution."

(Participant #8)

> "The challenge may be practical implementation and integration in real life business environment."

(Participant #25)

> "A good basis to identify insider threat. When customized and integrated with the existing system, it can help organizations be more proactive when dealing with threats from within."

(Participant #26)

Participant #3 said regarding the honeytoken component that "the honeypot technique is useful but could in my mind be more direct in trapping unauthorized access attempts".

Two participants added devices and technologies which the model should consider:

> "It should cover all aspects of communication gadgets like VoIP phones, fax, etc."

(Participant #5)

> “Need to consider all the newer stuff (IoT) devices, SCADIA, grid ageing internet, electromagnetic etc...”
>
> (Participant #7)

Participant #15 commented that there should be more explanations concerning user behaviours by stating, “a little more detail and context around user behaviours and what this would actually look like and how it would fit into an organizations strategy might be useful”.

Participant #21 urged that the privacy of the users should be preserved when collecting and storing the metadata so that it would not be open to abuse.

Some participants provided general recommendations on the model:

> “Try to add more variables and advanced algorithms to avoid too many false positives.”
>
> (Participant #16)

> “I believe that the system can include other Information security sections such as Awareness.”
>
> (Participant #20)

> “Expand the scope from targeting individual users to fight collusion.”
>
> (Participant #21)

> “The model should outline a potential roadmap. What are priorities and prerequisite on each component of the model?”
>
> (Participant #22)

6.4 Discussion of the findings

As it has been discussed in the data analysis, the components of the model have been well accepted receiving a rating above 70% by the participants. However, there is constructive feedback that has been forwarded by the participants, which will be used to further refine the model in the second iterations.

One of the parts of the motive component which has been severely criticized relates to the keyboard stroke analyser. Participants argue that the keyboard stroke analyser may result in false positives, as typing patterns may change due to factors like the passion of employees in different workplaces, the proficiency of the insiders in the language they use, the familiarity of the employees with the working environment and exceptional cases with professionals like coders.

As a solution to the problem related to false positives, some of the participants recommended a learning feature, which can be added to the component so that different scenarios will be considered, and the normal typing pattern will be learned. Similar criticisms related to false positives have raised issues with the resource usage analyser.

Considering the suggestions by the experts, a learning feature has been proposed to be included in the model, namely a pattern recognition model, using the Bayesian Network and the Hidden Markov model (HMM) to learn the normal behaviour of insiders in their typing pattern and resource usage. It is also able to detect any change in their stress levels and their resource usage behaviour so as to predict any risk factors for insider abuse.

The learning feature added to the model is very useful to learn the new behaviour of insiders. The research also suggests organizations to use continuous auditing to collect audit information in real-time using computerized tools so that they will detect any new fraudulent activities that deviate from normal behaviour in the model without delay. Continuous auditing has been studied by various researchers for its applicability to insider threat and found effective (Thomas & Marathe, 2012; Montelibano & Moore, 2012).

With regard to the opportunity component, it was suggested that the insiders' level of expertise should also be considered as one opportunity factor. However, the model considers assessing users' expertise as part of the capability component in user profiling since it is more related to the capability than the opportunity component of the model.

It has also been suggested by some of the participants to learn the behaviours of a user in terms of his/her capability, such as the motive component. This suggestion has also been included in the model.

There is also a suggestion that social media interactions of employees should be monitored to check whether they will use an opportunity to commit a crime however this will be in conflict with one of the objectives of the study, namely to preserve the privacy of insiders. The researcher accepts the recommendation of some of the participants that there should be an annual audit of administrators to assess opportunity but such actions should be done with respect to balancing their privacy.

Some of the participants raised a legal issue with regard to implementing honeytokens to monitor employees, as it is illegal in some countries. The researcher has suggested that organizations confirm the legality of all the components in this model before implementing it in their organizations. Honeytokens have also been criticized for breaching the privacy of employees and the researcher has suggested to organizations that they inform their employees that the organization will monitor their resource usage activities without including the contents of their communication to preserve their privacy.

Some respondents were concerned that honeytokens may turn honest users into perceived criminals, as insiders may interact with honeytokens without the intention of committing a crime. For this reason, the model considers other factors like motive and capability before labelling employees as at-risk insiders to reduce the chance of false positives. Nevertheless, the model is not punitive; it rather creates awareness about the organizations' information security policies.

Some of the participants have criticized the error and warning messages analyser of the capability component. They feel that it does not consider factors like the familiarity of the employee with specific versions of an application, frequency of errors in a short period of

time and a systems fault error. The researcher has accepted these suggestions and has modified the component to include a frequency of errors variable and to exclude system's fault errors. The component should work on an application with which a user is familiar so as to avoid any false positives due to a change in different versions of the same application. This may cause a user to make many errors due to unfamiliarity with the specific application.

Some of the participants have suggested that it is important to consider the training and the certification programs employees attend as well as books and manuals they have read. However, the researcher believes that the skills factor should be assessed continuously, as employees' skills change over time. The insiders' profiles can be updated to include their qualifications; however, the user sophistication component of the model to assess the employees' skills is done at run-time by assessing their current applications and other computer resources usage.

The importance of the capability component has been criticized as less important by one of the participants. He has justified his view by saying that committing a crime is easy and therefore does not require sophisticated IT skills. While the assertion may be true in some environments which do not have tight security systems, it still requires a certain amount of capability to abuse an information system equipped with a strong security system. Perhaps in some environments, the capability component could be disabled.

Some of the participants also recommended information security awareness to be added to the model. The remove-excuse techniques of the situational crime prevention theory is included within the neutralization mitigation component however it also creates an awareness of information security policies as part of removing excuses for any breach of the organizational policy as demonstrated in the prototype.

One participant suggested an expansion of the model from individual insider threats to collusion threats. Collusion threats refer to threats which occur when two or more individuals (insiders and/or outsiders) collaborate to commit a crime (Sogbesan, Ibidapo, Zavarsky, Ruhl & Lindskog, 2012). The researcher believes that the idea of including collusion threats is relevant however the Fraud Diamond theory on which forms the

cornerstone of this model is proposed based on the assumption that fraud is committed by individuals. The researcher recommends that future research investigate the application of the Fraud Diamond for collision detection which is a major research endeavour in itself. The lack of a mechanism to counter collusion is a limitation of the model.

6.5 Validity

To ensure the validity of the opinion of experts, the level of consensus on the concepts that are implemented in the model were tested. The conformity of the concepts with existing literature on insider threats and related areas is also verified. The validity of the experts' diversity is maintained by selecting participants from a variety of industries as well as different expertise levels in information security professions so as to obtain comprehensive feedback from the experts.

6.6 Chapter summary

This chapter presented a prototype and simulations to demonstrate a privacy-preserving, context-aware, insider threat prediction and prevention system, using the asset management system as a case study (see section 6.2). The prototype was based more on the user interface rather than the functionality of the model. The prototype was used to show the feasibility of the components of the model which include the context analyser, decision manager, honeytoken, user profiling, neutralization mitigation, situational crime prevention and a privacy-preserving filter. The chapter presented the feedback of the panel of ~~26~~ information security professionals (n=26) by using frequency counts as well as bar and pie charts to discuss the evaluation results (see section 6.3). A discussion of the findings of the experts was the input for the second iteration (see section 6.4). According to the evaluation of the first iteration, all of the components of the model rated above 70%.

The next chapter will discuss the evaluation of the second iteration.

CHAPTER SEVEN

EVALUATION: CYCLE II

7.1 Introduction

According to the principles of design science research, there is a need to evaluate the proposed artefact by using iterations until the artefact is refined in line with the standard. The feedback from experts in the first iteration required the model and the prototype to be revised after the panel of experts were presented with a second iteration. This chapter firstly discusses the revised model as well as the changes made to the prototype as per the expert opinions raised in the first iteration. Then the chapter presents and analyses the feedback of the panel of experts regarding their evaluation of the model in the second iteration and compares it with the results of the first iteration. Finally, the findings from the evaluation of the second iteration will be discussed.

7.2 Refined model

As mentioned in the discussion of the findings (section 6.4 above), the model was refined even further, based on the input that had been collected from the experts. The researcher has primarily added a learning feature to the motive and capability components, as per the recommendations of the experts. They suggested that unless the model learned the behaviours of insiders by taking into consideration different variables, it might result in a false positive. The researcher proposed the use of a pattern recognition model, such as the Bayesian Network, Hidden Bayesian Network, Hidden Markov model (HMM), to learn the normal behaviour of insiders to detect any deviation from their normal behaviour. The researcher also included more variables to the error and warning analyser, namely the familiarity of the employee with a specific version of an application, the frequency of errors within a short period of time, and a system's fault error based on the recommendations of the experts as shown in Figure 7.1.

The refined model is presented in Figure 7.1 with the addition of the learning component. After refining the model based on the recommendations put forward by the panel of experts, the researcher revised the questionnaire for experts and again presented the model for their evaluation. The questionnaire was designed to include learning feature in the components. A total of twenty-five experts (n=25) participated in the second iteration while one of the participants withdrew from the study due to personal reasons.

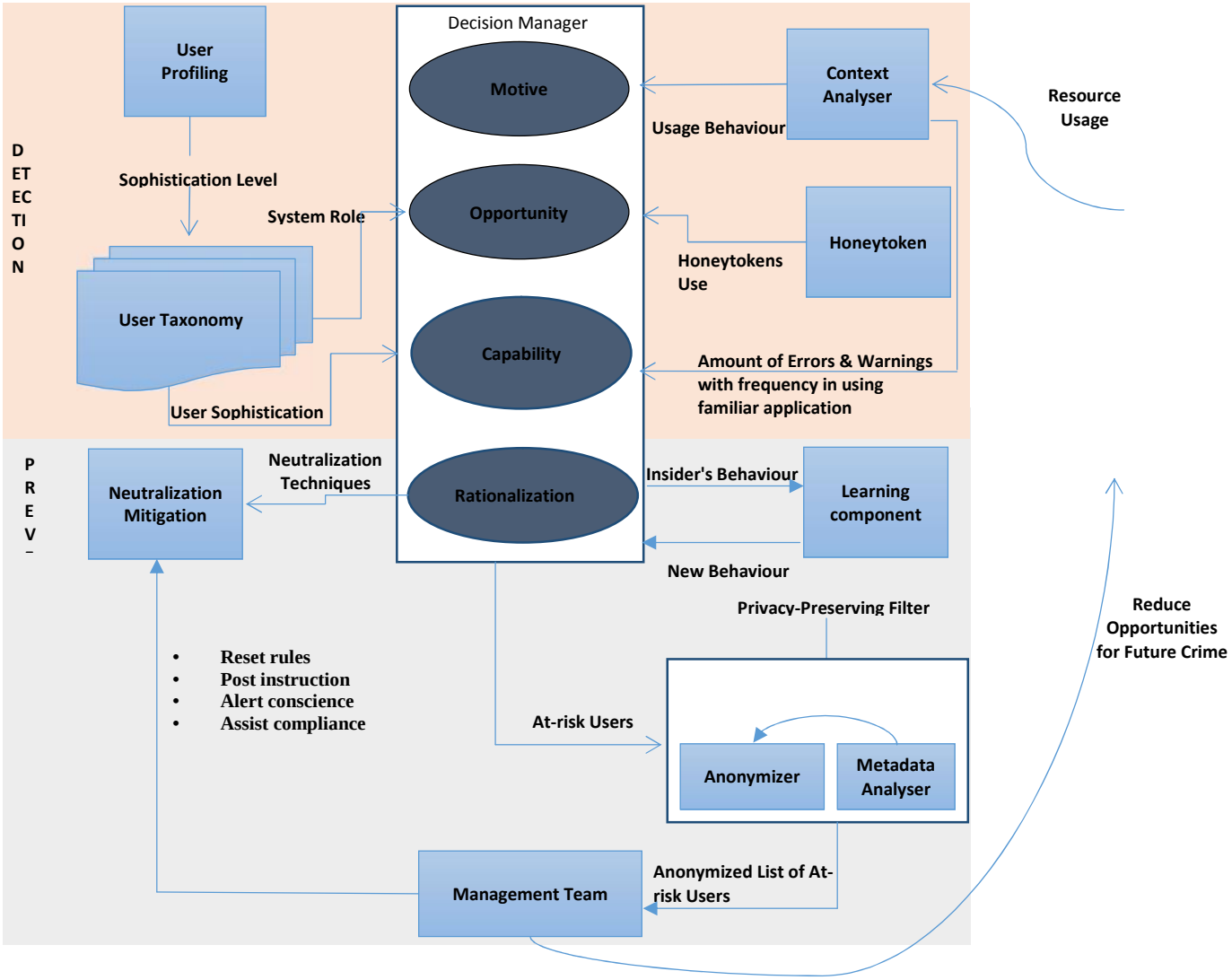

Figure 7.1 Refined model

7.3 Revised prototype

Based on the decision to include a learning component, the prototype is revised to demonstrate an example of learning behaviours. The report presented in Figure 7.2 depicts the output of new types of behaviours that are learned by the model. For instance, if the mouse press changes with stress, it will be reported as a new behaviour to be considered for the motive component. The prototype shows the possible user interface of the model implementation and is not a functional prototype.

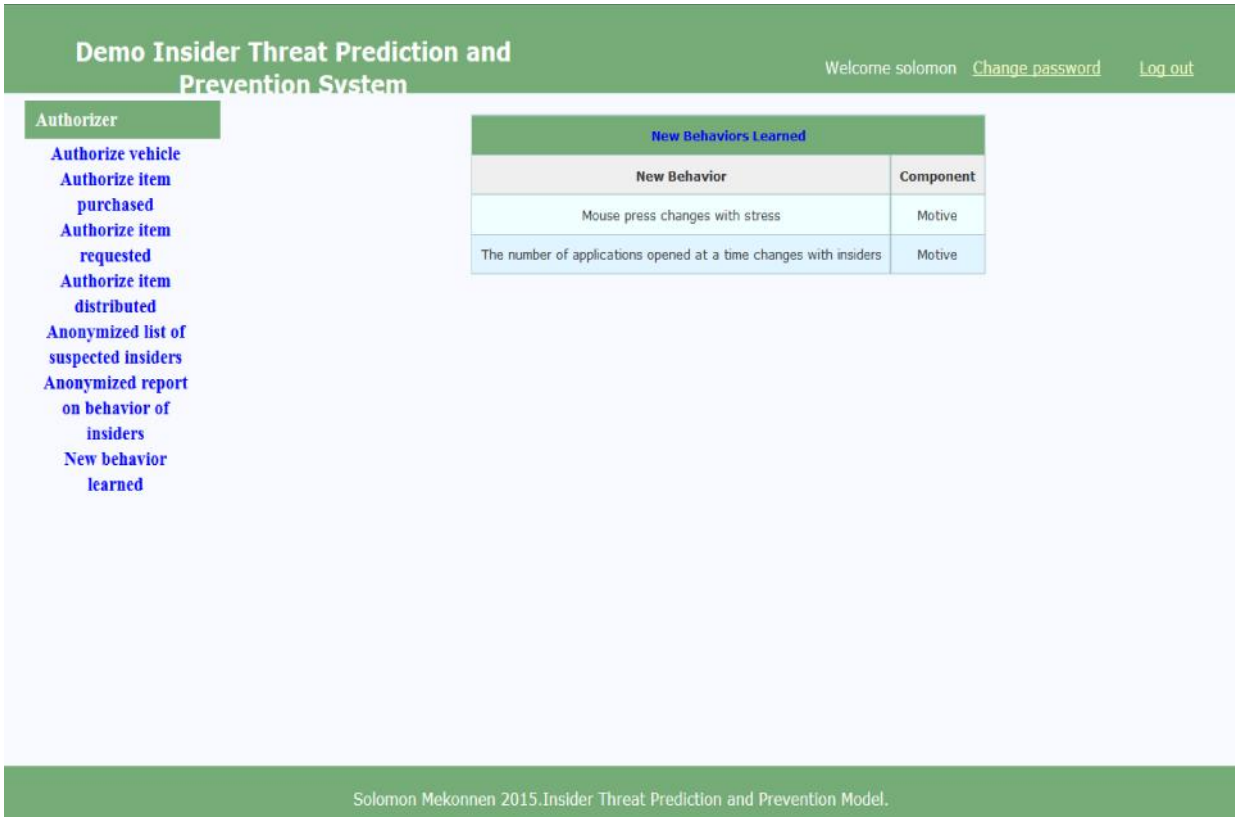

Figure 7.2 Interface: Report on new behaviours

7.4 Data analysis

All of the participants, except one who participated in the first iteration, also participated in the second iteration which brought the sample size to 25 (n=25). The participants were categorized into six categories based on their professional backgrounds and this is with seven information security supervisors (n=7), five information security engineers (n=5), five information security consultants (n=5), three information security analysts (n=3), three information security architects (3) and two information security specialists (n=2).

7.4.1 Results of the value judgments

As per the evaluation of the second iteration, all factors are rated above 75% with viability ranked the highest (94%) and usability (77%) ranked the lowest. Comparing the second iteration with the first iteration, the utility of the model is ranked at 88% which is an increase of 2% from the first iteration. It may be due to the "Learning new behaviour" feature the researcher has included in the motive and capability components of the model as well as the inclusion of considering frequency of errors to the error and warning analyser.

There is a 3% increase in the efficacy of the model in the second iteration which may be the result of including the learning component in detection of pressure. No other change notices in other variables of the value judgment were identified. The results of the study are presented in Figure 7.3.

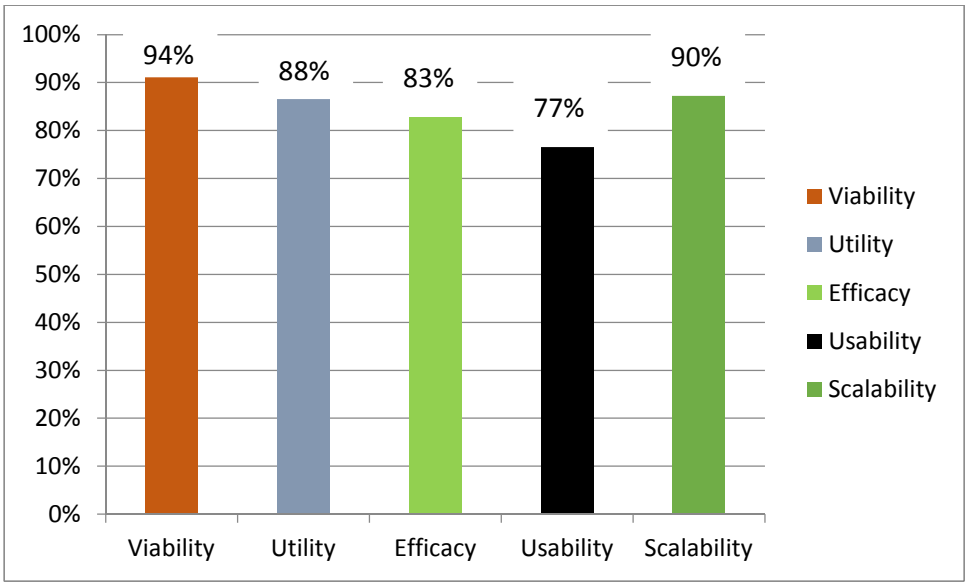

Figure 7.3 Value judgments for the second iteration

7.4.1.1 Viability

The viability of the model was ranked at 94% in the second iteration based on the factors of implementability and integrability which are the same as in the first iteration. Like the first iteration, 88% of the participants agreed that the model concept could easily be translated into an implementable product (Question 1). All of the participants agreed that the model could be easily integrated into the existing system (Question 5) which was also similar to first iteration.

7.4.1.2 Utility

In the second iteration, the utility of the model ranked at 88% which showed a 2% increase from the first iteration. Some improvement was observed in the utility of the reasonability of the model, the keyboard stroke analyser, the resource usage analyser and the error and warning messages analyser. The other components remained the same.

7.4.1.2a Utility in terms of general exploitation of the model concepts

Utility of the effects of the model in detection and prevention of insider threats

In the second iteration, 92% of the participants agreed that the model would support organizations' prediction and prevention of insider threats. The participants justified their views regarding the effects of the model in the detection and prevention of insider threats (Question 2). There was no change in the results from the first iteration.

Utility of the reasonability of the model

With respect to the reasonability of the model (Question 3), 83% of the participants agreed that the assumptions in the model were reasonable. Their responses showed an increase of 6% compared with the first iteration. The positive increase might be the result of including the learning feature in the motive and capability components of the model as well as improving the error and warning analyser.

Participant #14 supported his/her argument by stating: "As long everyone in the organization makes it his/her responsibility to protect organizational data yes the model would be very helpful as a guiding principle which will assist the total protection mechanism."

Utility of the benefit of the model for decision-making

As with the first iteration, 96% of the participants agreed that the proposed model can be used as a framework to aid organizations in information system security investment or development decision making processes to address the insider threat problem (Question 4).

7.4.1.2b Utility related to the motive component

Utility of the keyboard stroke analyser

With respect to the keyboard stroke analyser (Question 9), 80% of the participants agreed with the utility of the keyboard stroke analyser. This percentage increased by 3% from the first iteration. The positive increase might be as a result of adding the learning feature to the component.

Participant #21 added the following recommendation:

> "To be effective it has to be a standard monitoring process where necessary reviews are conducted to prove effectiveness, otherwise it would be like any other tool only implemented for compliance reasons without measurements of its worth to the organization."

Utility of the resource usage analyser

The utility of the resource usage analyser (Question 10) increased significantly by 8% to 88% in the second iteration as compared to the first iteration. This might result from including the "Learning new behaviour" feature to the component.

Participant #4 added the following caveat to his agreement:

> "Yes, searches at some point may reveal as to what subject of interest was to the insider conducting the searches and what download links where visited has to do to assist the insider towards achieving his malicious intents."

7.4.1.2c Utility related to the opportunity component

Utility of the effects of understanding opportunity in minimizing cybercrime

In terms of the benefit of understanding opportunities in minimizing crime (Question 11), all of the participants agreed that understanding the opportunities (e.g., weak access

controls) an insider may use to launch an attack would help in minimizing the risk of cybercrime. This result was analogous with the first iteration.

Utility of the level of access analyser

With respect to the utility of the level of access analyser (Question 13), 88% of the participants agreed that the level of access (i.e. systems role) granted to an insider (i.e. administrator, advanced user, novice) could be a means of identifying insiders who might be future threats to an organization's IT infrastructure. This result was the equivalent with the result of the first iteration.

7.4.1.2d Utility related to the capability component

Utility of a user's capability to use information systems

In terms of the capability of a user to use information systems of an organization (Question 14), 96% of the participants agreed that this component (i.e. user sophistication) could be a factor for insider threat mitigation, as users need to be capable of exploiting the organization's IT infrastructure in order to commit a cybercrime. This result was the equivalent with the result of the first iteration.

Utility of the error and warning message analyser

The utility of the error and warning message analyser (Question 15) was accepted by 84% of the participants in the second iteration, which showed a 3% increase from the first iteration. The improvement might be the result of the addition of more variables, including the number of errors and their frequency in a short period of time as well as making an assessment by means of an application software with which an employee was familiar.

Participant #22 provided the following remark in this regard: “Yes as long as this is monitored in a systematic manner.”

Utility of user profiling to determine the sophistication level

In terms of the utility of user profiling to determine the sophistication level (Question 16), 85% of the participants agreed that this component (i.e. capability) of insiders could be achieved by means of an examination to evaluate their knowledge with respect to computer usage (in terms of operating systems in use, techniques implemented, familiarity with specific technologies, etc.). There was no variation from the first iteration.

Utility of the insider capability analyser

With regard to the utility of the insider capability analyser (Question 17), 92% of the participants agreed that the capability of insiders could be verified, based on the types of applications they used and the level of computational resource usage consumed. This result was the equivalent to the results of the first iteration.

7.4.1.2e Utility related to the rationalization component

The utility of rationalization techniques

In terms of the utility of rationalization techniques (Question 18), 85% of the participants agreed that an understanding of rationalization techniques, which insiders might use to justify their crime, could be used to design a neutralization mitigation strategy to circumvent any excuse for committing a crime in future. This result was the equivalent to the results of the first iteration.

The utility of situational crime prevention techniques

There were no variations in the results for these questions from the first iteration.

Utility of setting rules

With respect to the utility of setting rules (Question 22), 96% of the participants agreed that setting rules (i.e. policy) which explicitly invalidated any potential defences (i.e. excuses) for cybercrime might be a useful mitigation strategy This result was the equivalent to the results of the first iteration .It implied that the rules should be reset based on new justifications for cybercrime.

7.4.1.2f Utility related to privacy preservation and the context analyser

Utility of Privacy Preserving

In terms of the utility of privacy preservation (Question 24), 73% of the participants agreed that collecting metadata only, such as search behaviour, file access, keystrokes and linguistic features, without collecting the content of employees' communication could help to balance privacy issues associated with insider threat detection. This result was similar to the results obtained in the first iteration.

Utility of the context analyser

With regard to the utility of the context analyser (Question 26), 81% of the respondents agreed that understanding the context of an insider by considering the elements of usage behaviour, stress levels and the rate of error and warning messages generated was a useful mechanism towards mitigating the insider threat. The result was consistent with the results obtained in the first iteration.

7.4.1.3 Efficacy

In the second iteration, the efficacy component of the model was ranked at 83%. There was thus a 3% increase in the efficacy rating of the model in the second iteration. This is due to the result of including a learning component in the detection of pressures. The

increase was based on the efficacy of detecting the pressures, the efficacy of honeytokens and the efficacy of anonymization.

Efficacy of the detection of pressures

With respect to the efficacy of detecting pressures (Question 8), 88% of the participants agreed on this factor (e.g. anger, frustration or despair due to organizational factors such as denial of salary increases or personal problems) could motivate insiders to commit maleficence and it would be an effective means of insider threat mitigation. The results showed an increase of 7% from the first iteration which is due to the addition of the learning component

Participant #20 remarked: “Absolutely if new behaviours are learned, these are some of the factors that can motivate insiders to commit malicious intents to the organization, a list goes on and on.”

Efficacy of honeytokens

In terms of the efficacy of honeytokens (Question 12), 77% of the participants agreed that deploying honeytokens (i.e. deception traps to lure insiders) by means of extraneous links, fake information on a database etc. was an effective technique to identify future threats. This result is consistent with the first iteration.

Efficacy of anonymization

With regard to the efficacy of anonymization (Question 25), 88% of the participants agreed that anonymization (i.e. removing identifiers) was an effective technique to protect individuals’ identity when releasing sensitive information about potential insider threats. This result is consistent with the first iteration.

7.4.1.4 Usability

In terms of usability (Question 23), 77% of the participants agreed that insider threat prevention and detection strategies should not infringe upon the privacy of insiders. This result is consistent with the first iteration.

7.4.1.5 Scalability

The scalability of the model was ranked at 90%, which depended on the practicality, applicability and the model concept. This result is consistent with the first iteration.

7.4.1.6 Practicality

With regard to practicality (Question 6), 84% of the participants agreed that the model would be scalable in a real-world context. This result is consistent with the first iteration.

7.4.1.7 Applicability

With respect to applicability (Question 7), 96% of the participants disagreed that there were no conceivable environments in which this product concept would be applicable. This result is consistent with the first iteration.

7.5 Discussion of findings

After refining the model based on the participants' feedback from the first iteration, there were some improvements in the evaluation of the model in the second iteration.

The utility of the model was ranked at 88% in the second iteration, which showed an increase of 2% from the first evaluation. This is due to the result of adding a new learning component to the model as well as modifying the error and warning message analyser.

The efficacy of the model also showed an increase of 3% from the first iteration which is the result of the addition of a learning feature in detecting the motive of insiders.

There was also an improvement in the evaluation of the reasonability of the model which increased by 6% in the second iteration. It is due to the result of including a learning

feature in the motive and capability components of the model as well as improving the error and warning message analyser.

The components of the keyboard stroke analyser and the resource usage analyser increased by 3% and 8% respectively which is also the result of including the learning component in the model.

There was an increase of 3% in the evaluation of the error and warning message analyser. This is also the result of including frequencies of errors in a short period of time as well as making assessments by using an application with which the employees were familiar.

There was no significant feedback from the experts in the second iteration which required further refinement of the model.

7.6 Validity

To ensure the validity, the data from both iterations were triangulated. The experts verified the revised model and also provided supplementary feedback in the second iteration as confirmation. The heterogeneity of the experts in terms of representation from different information security fields was maintained by selecting experts from a wide variety of industries, each with his/her own field of expertise. To ensure the validity of the experts' opinions in the second iteration the level of consensus and conformity with existing literature was verified.

7.7 Chapter summary

This chapter discussed the changes made to the model as well as to the prototype, based on the expert opinions provided in the first iteration (see section 7.2 and section 7.3). Subsequently, the results of the evaluation for the second iteration were discussed in detail and compared to the findings of the first iteration to show the variations (see section 7.4). A panel of information security experts (n=25) participated in the second

iteration of the study. The results of their feedback were presented by making use of frequency counts as well as bar and pie charts. Finally, the findings from the second iteration were discussed by drawing a comparison with the results of the two respective iterations (see section 7.5). According to the evaluation of the experts in the second iteration, all of the components of the model were rated above 80% except usability (77%) which is a positive indication.

The next chapter will provide a summary of the research, its findings and contributions, future research areas and conclusions drawn from the study.

CHAPTER EIGHT

CONCLUSIONS, IMPLICATIONS AND FUTURE RESEARCH

8.1 Introduction

This chapter concludes with a summary of the research and future research avenues. The overview of the study summarizes the research presented in section 8.2. Section 8.3 discusses the research questions identified at the beginning of the research and how the questions are answered in the study. The contributions the study has made towards both the scientific body of knowledge as well as information security practitioners in the industry are discussed in section 8.4. The limitations of the study are discussed in section 8.5. Section 8.6 considers future research avenues. Finally, the conclusions drawn from the research are discussed.

8.2 Overview of the study

In order to determine the extent to which the components of the Fraud Diamond could be effective in predicting and preventing the insider threat using contextual information while preserving privacy, a research project was designed that posed a central question: *How approaches from the disciplines of criminology and computer science could be integrated into a feasible model that would address the insider threat problem.* This research proposed a novel **P**rivacy-**P**reserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction (PPCAITPP) model, integrating approaches from the disciplines of computer science and criminology.

The model proposed in this research is predicated on the Fraud Diamond, which argues that four factors need to be present for an insider to commit a crime, namely motive, capability, opportunity and rationalization. The model preserves the privacy of insiders.

Hence, the content required to assess elements of the Fraud Diamond is not collected; rather the contextual type information is collected at a meta-level based on metadata, which includes search behaviour, file access, logins, using keystrokes and linguistic features. All information about insiders is anonymized to remove any identifiers that may be used to uniquely identify insiders so that their privacy remains protected. Privacy is very important because unless it is preserved, it may frustrate employees and result in future insider threats. In some countries, the privacy of employees in the workplace is legally protected. The model uses a context-aware analyser to determine the motive of insiders based on the metadata. The context analyser is used to assess the capability of insiders based on the number of errors and warnings generated while they use an application, and it combines this component with user sophistication. The model also identifies new behaviours related to the motive and capability of insiders. Once the motive and capability of the insiders have been assessed, the model presents the list of at-risk insiders to the management team and they then decide to provide the insiders with an opportunity by means of honeytokens to commit a crime. If the insiders access the honeytoken, the model implements neutralization mitigation to remove any excuse for the malicious act and alerts the insiders through situational crime prevention techniques.

The model was demonstrated in the form of a prototype, which uses an asset management system as a case study, as insiders usually commit malicious acts at the application level. Both the model and the prototype were presented to a panel of information security experts for evaluation as per the guidelines of design science research. The experts evaluated the model and the prototype based on its viability, utility, efficacy, usability and scalability. Its research rigour is based on the four principles of design science research, namely abstraction, originality, justification and benefit. The evaluation was conducted in two iterations with all components of the model rated above 80% except usability (77%) by the experts.

8.3 Achieving the research objectives

The main objective of this research was to develop a **P**rivacy-**P**reserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction (PPCAITPP) model (see section 1.5.1). As stated in extant research, the main research findings of the design science research are the development of artefacts which include constructs such as concepts, terminologies and languages as well as models, methods and instantiations (i.e. concrete solutions implemented as prototypes or production systems) (see section 4.3). Thus, the main contribution of this research is the artefact itself designated the **P**rivacy-**P**reserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction model (see chapter five). The artefact was demonstrated by means of a user interface (UI) prototype, functional prototypes and simulations (see section 6.2 and section 7.3).

In the process of developing the artefact, the research study answered the five research questions identified at the beginning of the research (see section 1.4). The findings are discussed below. The achieved objectives of the study were directed by the following research questions:

> Main research question: How can approaches from criminology and computer science be integrated into a feasible model that will address the insider threat problem?
>
> RQ1: To what extent can the components of the Fraud Diamond be feasibly applied to address the insider threat problem?
>
> RQ2: To what extent can the physical and virtual contexts be used to predict an insider threat?
>
> RQ3: To what extent can the privacy of insiders be preserved by an insider threat prevention and prediction model?
>
> RQ4: To what extent is the proposed model effective in preventing and detecting insider threats?

Main research question (How can approaches from criminology and computer science be integrated into a feasible model that will address the insider threat problem?)

The issue of insider threat problems is complicated, as insiders are people who display unique and changing behaviours which make it challenging to predict their actions and to mitigate any risks posed by these insiders. Firstly, the behavioural component of insiders requires considering approaches from the field of psychology to detect stress and emotions related to a motive. Secondly, insiders working in the cyber security domain share similar characteristics with other insiders involved in physical crime; therefore, there is a need to borrow theories from the field of criminology as well. Thirdly, since this research focuses on insider threats in the cyber security domain, there is a need to consider solutions from the field of computer science.

This research has investigated the application of the Fraud Diamond, situational crime prevention, neutralization mitigation, the psychological factors for committing a crime from the field of psychology and a context-aware system from the field of computer science (see chapter three and chapter five). The integration of these approaches is validated as effective and efficient by the panel of information security experts who have participated in this study (see chapter six and chapter seven). The success in this study can be replicated by other researchers in dealing with insider threat problems.

RQ1 (To what extent can the components of the Fraud Diamond be feasibly applied to address the insider threat problem?)

According to Bressler and Bressler (2007), there should be four elements in order for fraud to be committed, namely pressure, opportunity, rationalization and capability. The authors have coined these components as the Fraud Diamond. There is research available which has investigated the mapping of the Fraud Diamond to the insider threat problem under the hypothesis that insiders share similar characteristics with other fraudsters. The mapping of the Fraud Diamond to the insider threat problem has been presented to a panel of information security experts and was well accepted by the panel (see chapter six

and chapter seven). The output of this research could also be used by other researchers to investigate further applications of the Fraud Diamond to the insider threat problem. The mapping of the components of the Fraud Diamond, namely motive, capability, opportunity and rationalization are discussed next.

a. ***Motive:*** A context analyser is used to collect information related to an insider who may be motivated to commit a crime through resource usage behaviour. The model employs keystroke and linguistic features based on the insider's typing patterns to collect information about any change in the insider's emotions and stress levels, which are indirectly related to his/her motivation to commit a cybercrime.

b. ***Capability:*** The model assesses the capability of insiders to commit a planned attack based on their usage of computer applications and measuring their sophistication in terms of the range of knowledge, depth of knowledge and skill as well as assessing the number of systems errors and warnings generated while using the applications.

c. ***Opportunity:*** The model will facilitate an opportunity to commit a crime by implementing honeypots to determine whether a motivated and capable insider will exploit any opportunity in the organization to become involved in a criminal act.

d. ***Rationalization:*** Based on the insider's reaction to the opportunity presented via a honeypot, the model deploys an implementation strategy by means of neutralization mitigation to nullify the rationalizations the insider may have had for committing the crime.

RQ2 (To what extent can the physical and virtual contexts be used to predict an insider threat?)

The changing behaviour of insiders makes it challenging to predict who the insiders are and to prevent them from committing a crime. The challenge requires the application of

techniques that need to assess the current behaviour of insiders automatically to avoid any false positives with predictions due to changing behaviour of the insiders.

This research also demonstrated the application of the typing pattern analyser to assess the physical contexts like stress levels and emotions related to the motive of insiders to commit a crime (see section 3.4 and section 5.3.1.1a). Their virtual contexts like search behaviour, file access, and login are assessed by making use of the resource usage behaviour analyser. Therefore, this research has investigated the application of a context-aware system to gather contextual information in real-time as it relates to the motives and capabilities of insiders so as to assist their prediction (see section 5.3.1.1a). The approach was well accepted by the panel of information security professionals during their evaluation of the model (see chapter six and chapter seven).

The concept of a context-aware system has been used to leverage the following dimensions and interactions:

a. ***Motivation:*** by monitoring the interactions with the system (i.e. considering metadata such as search behaviour, file access, logins and keystrokes)

b. ***Capability:*** by monitoring systems warnings and errors, and the insiders' usage of computer applications to measure their level of sophistication in terms of the range of knowledge, depth of knowledge and skill.

c. ***Opportunity:*** by monitoring the insiders' interactions with the honeytoken which has been deployed to identify suspicious insiders

d. ***Rationalization:*** by monitoring the suspicious insiders' interactions with the neutralization mitigation analyser to identify and nullify their justifications in order to prevent future crime.

RQ3 (To what extent can the privacy of insiders be preserved by an insider threat prevention and prediction model)

One of the critiques of information security solutions dealing with an insider threat is that the solutions are mainly based on workplace monitoring which may result in stress, low commitment and even lower productivity levels (Brown, 1996; Dhillon & Moores, 2001). To address this problem, this study has investigated the use of metadata such as search behaviour, file access, logins, using keystrokes, linguistic features and the number of errors and warnings given the insiders without collecting contents to assess their motives and capabilities; thus, preserving their privacy (see section 5.23 and section 5.33). Even the metadata is anonymized to remove any identifiers of a specific insider. The approach was well accepted by the panel of information security experts (see chapter six and chapter 7).

The privacy-preserving technique that has been used in this research could also be used by other researchers to address insider threat problems. The model preserves the privacy of the insiders in the following ways with respect to each dimension:

a. ***Motivation:*** The motivations of an insider are not identified; rather the metadata associated with an insider who is motivated to commit a cybercrime is collected.

b. ***Capability:*** The insider's capability is assessed in terms of his/her usage of computer applications without uniquely identifying the individuals.

c. ***Opportunity:*** The honeytokens are deployed anonymously to suspicious insiders.

d. ***Rationalization:*** The information from the neutralization mitigator is done anonymously.

RQ4 (To what extent is the proposed model effective in preventing and detecting insider threats?)

One of the challenges of insider-threat research is evaluating the research output. It is particularly challenging to obtain insiders' data, as organizations do not make it public

because of its effect on the reputation of the organization as well as privacy and ethical issues.

To tackle this challenge, this research has employed different techniques to evaluate the artefact/model, namely expert evaluation, a prototype and a simulation based on the principles of design science research (see chapter six and chapter seven). According to the expert evaluation, the model was accepted by the expert panel and the components of the model are rated above 80% except for usability (77%) (See chapter seven). As per the feedback from the expert panel, the model was found to be acceptable towards aiding organizations in making investment decisions related to acquiring solutions that address the insider threat problem.

The model also helps information security practitioners in designing and developing security solutions to mitigate insider threats. The artefact proposed in this research, which is a **P**rivacy-**P**reserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction (PPCAITPP) model, is a novel model which contributes new knowledge to the field of information security research (see chapter five).

8.4 Contributions of the study

8.4.1 Theoretical contributions

According to Österle et al. (2011), "the main contributions of design science research are the development of artefacts. These include constructs (e.g. concepts, terminologies and languages), models, methods and instantiations (i.e. concrete solutions implemented as prototypes or production systems)" (p.8). Therefore, the main contribution of this thesis is the artefact itself, namely the **P**rivacy-**P**reserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction model. While developing the model, other contributions like research results of this study have come to the fore. Each contribution is discussed below.

Contribution 1 (The artefact – A privacy-preserving, context-aware, insider threat prediction and prevention (PPCAITPP)) model

This study has produced a **P**rivacy-**P**reserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction (PPCAITPP) model which has been validated to address the insider threat problem by combining different approaches from the disciplines of computer science and criminology. The model was based on prior research to insider threats and other related disciplines as per the guidelines of design science research. In addition, expert opinions have been collected from a panel of experts in two iterations in order to improve as well as validate the artefact/model. Moreover, the artefact has been demonstrated practically with a prototype and presented to this panel of experts for evaluation. They followed the guidelines of design science research in their evaluation and they accepted the model.

Contribution 2 (Integration of approaches from computer science and criminology)

Information systems are designed and implemented to be used by people and therefore human factors should be considered in the design as well as their implementation of the systems.

The focus of this study is insider threats, and as insiders are people with their own psychological characteristics, it requires an investigation of psychological approaches to address the issue of insider threats. Although this research focuses on insider threats in the cyber security domain, there are similarities with criminology solutions in the physical domain because in both cases we deal with human perpetrators. Thus, there is a need to investigate approaches from the field of criminology to address the insider threat problem. This research has laid a foundation for the way in which different approaches from the disciplines of computer science and criminology can solve security problems in information systems.

Contribution 3 (The application of the Fraud Diamond to insider threats)

Bressler and Bressler (2007) have proposed the Fraud Diamond with the hypothesis that there are four conditions to be present in order for fraudsters to commit a crime. These are pressure, opportunity, rationalization and capability. The model has proposed techniques to identify any type of fraudsters, as there are similarities with insiders who also commit crimes. One should keep in mind that fraud is also a type of insider threat.

This research has demonstrated the mapping of the Fraud Diamond for insider threats and is open to other researchers to further investigate the application of the Fraud Diamond in the information security domain.

Contribution 4 (The application of a context-aware system to insider threats)

The main focus of this study is the issue of insider threats with the main actors being insiders in organizations. The behaviour of insiders is dynamic and therefore it is difficult to predict insiders' behaviour. The reason is that every person has his or her own unique and complex behaviour which changes periodically.

Depending on the questionnaires filled out by the insiders themselves on their behavioural indicators and information that is available on human resources, databases are not reliable. The reason is that dynamic changes occur in human behaviour and employees may also not be truthful when providing information about themselves. Their managers/supervisors may be biased and not provide truthful information about the employees to human resource experts.

The problems discussed above require investigation into the automatic collection of data on the current behaviour of insiders. This research demonstrates that a context-aware system can be used to automatically collect current information about the behaviour of insiders, and it can also be used for predicting at-risk insiders.

Contribution 5 (Preserving the privacy of insiders)

Information security systems which conduct workplace monitoring without preserving the privacy of employees may result in stress, low commitment and even lower productivity levels (Brown, 1996; Dhillon & Moores, 2001). Insider threat solutions should, therefore, consider balancing the privacy of employees if monitoring is involved.

This research has demonstrated how the necessary information for the prediction and prevention of insider threats can be collected and used without infringing on the privacy of insiders. This is possible by collecting only metadata about insiders such as their search behaviour, file access, logins, keystroke use and linguistic features without collecting the content in order to balance the privacy issue. The metadata is anonymized (i.e. all identifiers are removed) so as to avoid any risk of being abused by intruders.

8.4.2 Practical contributions

The model proposed in this research can be used by organizations as a framework to make any investment decisions related to information security systems and infrastructure to address the issue of insider threats. Information security practitioners could also design and develop information security systems to address insider threats, based on the concepts implemented in the model presented in this study. This model can also be used as a reference by other forensic experts like forensic accountants as their role is to detect fraud in organizations based on their accounting, auditing and investigative skills. Forensic accountants are playing a major role in detecting fraudsters in countries like the United States saving $600 billion on theft and fraud per year (Özkul & Pamukçu, 2012). The model can also be used to improve existing information security systems to mitigate insider threats, based on the theoretical ideas that are included in the model. The model presented in this study may also be used as a reference to develop any general information security system not specific to insider threats, as the concepts could also be adopted for other areas of cybercrime.

8.5 Limitations of the study

The sample size of the panel of experts (n=26 in the first iteration and n=25 in the second iteration) who have evaluated the model and the prototype is relatively small which might be considered a limitation of this study. Over 260 information security experts were invited to participate in this study and the response rate was 10%. The participants were selected purposively by the researcher, based on their expertise and their experience in information security which might bias the research. As a demonstration, some parts of the model, like user sophistication, were demonstrated by using the interface prototype. This might not show the full functionality of the prototype and could be considered another limitation of this study. This study was carried out with the assumption that an insider would commit a crime individually and did not anticipate those crimes committed by groups of insiders, which are called collusion threats.

8.6 Future research

The insider threat problem is complex and far-reaching; therefore, this research study could not cover all the issues in this regard. It is envisaged that appropriate themes for future research may include the following:

- This study has focused on individual insider threats, excluding collusion threats. Collusion threats refer to those threats that occur when two or more individuals (insiders and/or outsiders) collaborate to commit a crime (Sogbesan et al., 2012). Expanding the model proposed in this research to include collusion threats would be an interesting research area for further exploration.

- The model proposed in this research is a general one. There may be issues like legality and cultural aspects in adapting this model to specific countries, which might be another research area.

- The model proposed in this research uses metadata like search behaviour, file access, logins, keystroke usage, linguistic features and errors, and warnings,

excluding content to balance the privacy of insiders. Though the use of metadata significantly preserves the privacy of insiders it cannot be avoided completely, as monitoring the metadata will, to some degree, affect the privacy of insiders. Investigations into other sources of data for monitoring insiders and at the same time preserving their privacy is another area requiring further investigation.

- This research has employed neutralization mitigation and situational crime prevention as techniques for the prevention of insider threats by removing any excuse for crime. Researchers may investigate other prevention techniques like crime prevention through environmental design (CPTED), developmental crime prevention as well as repeat victimization and evidence-based crime prevention to be applied in detecting insider threats.

- This study used the anonymization technique to remove identifiers from metadata collected so as to preserve the privacy of insiders. There are also other techniques for privacy-preserving which include the randomization method and the distributed privacy-preservation technique. Investigating different privacy techniques that are applicable to insider threats and making comparisons can also be another area of research.

- The model proposed in this study has been evaluated based on its pilot application (prototype) and expert reviews. However, there are other evaluation techniques in design science research such as laboratory experiments and field experiments (Österle et al., 2011) that may be useful in future research projects. Evaluating and testing the model with other techniques in design science research can be an additional research area.

8.7 Conclusions

This research has attempted to address the challenging and complex insider threat problem when insiders are trusted and authorized to access the information resources of an organization and then utilize these resources to commit a crime. The human nature and

behaviours of insiders are also complicated aspects to address, as insiders hail from diverse backgrounds. Their behaviour can change dynamically and contextually in different environments because of this diversity.

The issue of preserving the privacy of insiders while attempting to mitigate insider threats might result in future insider threats. Therefore, the complexity of insider threats requires investigating different theories from the disciplines of criminology and computer science to address this problem. This study has proposed a novel **P**rivacy-**P**reserving, **C**ontext-**A**ware, **I**nsider **T**hreat **P**revention and **P**rediction (PPCAITPP) model in combining approaches from the disciplines of criminology and computer science based on extant literature.

The proposed model has been demonstrated by using the prototype as well as simulation techniques. It was presented for evaluation to a panel of experts in information security systems, based on the principles of the design science research methodology. The panel accepted the model and they have rated the components of the model above 80% except usability (77%) on average.

The proposed model is a new contribution to the body of scientific knowledge in the information security domain, as it investigates and justifies the application of different theories from the fields of criminology and computer science to mitigate insider threats.

The model can be used by information security practitioners to make investment decisions in information security in mitigating insider threats. It can also be used as a framework to design and develop information security systems to address the insider threat problem.

REFERENCES

Adomavicius, G., Bockstedt, J. C., Gupta, A., & Kauffman, R. J. (2008). Making sense of technology trends in the information technology landscape: A design science approach. *MIS Quarterly*, 779-809.

Agrafiotis, I., Erola, A., Happa, J., Goldsmith, M., & Creese, S. (2016, May). Validating an insider threat detection system: A real scenario perspective. *Security and Privacy Workshops (SPW)*, 286-295. IEEE.

Ahmed, A., Latif, R., Latif, S., Abbas, H., & Khan, F. A. (2018). Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment: A Systematic Literature Review. *Multimedia Tools and Applications*, 1-19.

Albrecht, W. S., Wernz, G. W., & Williams, T. L. (1995). *Fraud: Bringing light to the dark side of business*. Burr Ridge, Ill: Irwin Professional Pub.

Ali, A., Ahmed, M., Ilyas, M., & Küng, J. (2017, November). MITIS-An Insider Threats Mitigation Framework for Information Systems. In *International Conference on Future Data and Security Engineering* (pp. 407-415). Springer, Cham.

Almehmadi, A., & El-Khatib, K. (2017). On the possibility of insider threat prevention using intent-based access control (IBAC). *IEEE Systems Journal*, *11*(2), 373-384.

Al-Muhtadi, J., Ranganathan, A., Campbell, R., & Mickunas, M. D. (2003, March). Cerberus: A context-aware security scheme for smart spaces. In *Pervasive Computing and Communications*, 2003. (PerCom 2003). Proceedings of the First IEEE International Conference. pp. 489-496. IEEE.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behaviour*, *49*, 567-575.

Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. *Procedia Computer Science*, 45, 436-445.

An, G., Bae, G., Kim, K., & Seo, D. (2009, December). Context-aware dynamic security configuration for mobile communication device. In *New Technologies, Mobility and Security (NTMS)*, 2009. 3rd International Conference. pp. 1-5. IEEE.

Anagnostakis, K. G., Sidiroglou, S., Akritidis, P., Xinidis, K., Markatos, E. P., & Keromytis, A. D. (2005, August). Detecting Targeted Attacks Using Shadow Honeypots. Proceeding of 14th USENIX Security Symposium, Baltimore, M.D. pp.129-144.

Anandarajan, A., & Kleinman, G. (2011). The impact of cognitive biases on fraudulent behaviour: The Leeson case. *International Journal of Behavioural Accounting and Finance*, 2(1), 40-55.

Ancona, M., Bronzini, B., Conte, D., & Quercini, G. (2012). Developing Attention-Aware and Context-Aware User Interfaces on Handheld Devices. In *Interactive Multimedia*. InTech.

Anderson, R. H. & Brackney, R. C. (2004). Understanding the Insider Threat. Proceedings of a March 2004 Workshop. RAND CORP SANTA MONICA CA.

Anderson, R. H., Bozek, T., Longstaff, T., Meitzler, W., & Skroch, M. (2000). Research on mitigating the insider threat to information systems-# 2 (No. RAND-CF-163-DARPA). Rand National Defence Research Inst Santa Monica CA.

Aquino, K., Tripp, T. M., & Bies, R. J. (2001). How employees respond to personal offense: the effects of blame attribution, victim status, and offender status on revenge and reconciliation in the workplace. *Journal of Applied Psychology*, 86(1), 52.

Aquino, K., Tripp, T. M., & Bies, R. J. (2006). Getting even or moving on? Power, procedural justice, and types of offense as predictors of revenge, forgiveness, reconciliation, and avoidance in organizations. *Journal of Applied Psychology*, 91(3), 653.

Araújo, L. C., Sucupira, L. H., Lizarraga, M. G., Ling, L. L., & Yabu-Uti, J. B. T. (2005). User authentication through typing biometrics features. *IEEE Transactions on Signal Processing*, 53(2), 851-855.

Archer, L. B. (1964). *Systematic method for designers*. London: Council of Industrial Design.

Arulampalam, M. S., Maskell, S., Gordon, N., & Clapp, T. (2002). A tutorial on particle filters for online nonlinear/non-Gaussian Bayesian tracking. *IEEE Transactions on signal processing*, *50*(2), 174-188.

Avison, D. E., & Myers, M. D. (1995). Information systems and anthropology: and anthropological perspective on IT and organizational culture. Information Technology & People, 8(3), 43-56.

Axelrad, E. T., Sticha, P. J., Brdiczka, O., & Shen, J. (2013, May). A Bayesian network model for predicting insider threats. *Security and Privacy Workshops (SPW)*, 82-89. IEEE.

Babu, B. M., & Bhanu, M. S. (2015). Prevention of insider attacks by integrating behaviour analysis with risk based access control model to protect cloud. *Procedia Computer Science*, 54, 157-166.

Baracaldo, N., Palanisamy, B., & Joshi, J. (2017). G-sir: an insider attack resilient geo-social access control framework. *IEEE Transactions on Dependable and Secure Computing*.

Bariff, M. L., & Ginzberg, M. J. (1982). MIS and the behavioural sciences: research patterns and prescriptions. *ACM SIGMIS Database*, 14(1), 19-26.

Baskerville, R. L., & Myers, M. D. (2002). Information systems as a reference discipline. *MIS Quarterly*, 1-14.

Beebe, N. L., & Rao, V. S. (2005, December). *Using situational crime prevention theory to explain the effectiveness of information systems security.* Proceedings of the 2005 Software Conference, Las Vegas, NV. pp. 1-18.

Bellovin, S. M. (2008). The insider attack problem: Nature and scope. *Insider Attack and Cyber Security*, 1-4. Springer US.

Benbasat, I., & Zmud, R. W. (1999). Empirical research in information systems: the practice of relevance. *MIS Quarterly*, 3-16.

Benbasat, I., & Zmud, R. W. (2003). The identity crisis within the IS discipline: Defining and communicating the discipline's core properties. *MIS Quarterly*, 183-194.

Bichler, M. (2006). Design science in information systems research. *Wirtschaftsinformatik*, 48(2), 133-135.

Bishop, M., Conboy, H. M., Phan, H., Simidchieva, B. I., Avrunin, G. S., Clarke, L. A., Osterweil, L.J., & Peisert, S. (2014, May). Insider threat identification by process analysis. *Security and Privacy Workshops (SPW)*, 251-264. IEEE Xplore Digital Library.

Bishop, M., Engle, S., Frincke, D. A., Gates, C., Greitzer, F. L., Peisert, S., & Whalen, S. (2010). A risk management approach to the "insider threat". In *Insider threats in cyber security* (pp. 115-137). Springer, Boston, MA.

Boender, J., Ivanova, M. G., Kammüller, F., & Primiero, G. (2014, July). Modeling human behaviour with higher order logic: Insider threats. In *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on* (pp. 31-39). IEEE.

Bowen, B., Salem, M. B., Hershkop, S., Keromytis, A., & Stolfo, S. (2009). Designing host and network sensors to mitigate the insider threat. *IEEE Security & Privacy*, 7(6), 22-29.

Bowen, B. M., Salem, M. B., Keromytis, A. D., & Stolfo, S. J. (2010). Monitoring technologies for mitigating insider threats. In *Insider Threats in Cyber Security* (pp. 197-217). Springer, Boston, MA.

Baracaldo, N., & Joshi, J. (2012, June). A trust-and-risk aware RBAC framework: tackling insider threat. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies* (pp. 167-176). ACM.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours.

Branscomb, A. W. (1994). *Who owns information? From privacy to public access.* Basic Books.

Brancik, K. (2007). Insider computer fraud: an in-depth framework for detecting and defending against insider IT attacks. CRC Press.

Bressler, M. S., & Bressler, L. A. (2007). A model for prevention and detection of criminal activity impacting small business. *The Entrepreneurial Executive*, 12, 23.

Brown, W. S. (1996). Technology, workplace privacy and personhood. *Journal of Business Ethics*, 15(11), 1237-1248.

Brown, P. J., Bovey, J. D., & Chen, X. (1997). Context-aware applications: From the laboratory to the marketplace. *IEEE Personal Communications*, 4(5), 58-64.

Brown, C. R., Watkins, A., & Greitzer, F. L. (2013, January). Predicting insider threat risks through linguistic analysis of electronic communication. In *System Sciences (HICSS)*, 2013. 46th Hawaii International Conference. pp. 1849-1858. IEEE.

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behaviour*, *68*, 190-209.

Byers, B., Crider, B. W., & Biggers, G. K. (1999). Bias crime motivation: A study of hate crime and offender neutralization techniques used against the Amish. *Journal of Contemporary Criminal Justice*, *15*(1), 78-96.

Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., & Willke, B. J. (2008). *Management and education of the risk of insider threat (MERIT): System dynamics modeling of computer system sabotage*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud)*. Addison-Wesley Professional.

Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. (2009). Common sense guide to prevention and detection of insider threats. 3rd edition. Version 3.1. CERT, Software

Engineering Institute, Carnegie Mellon University PA, USA. [online]. Available at: http://www.cert.org (Accessed: 15 June 2017).

Caputo, D., Maloof, M., & Stephens, G. (2009). Detecting insider theft of trade secrets. *IEEE Security & Privacy*, 7(6), 14-21.

Centre for the Protection of National Infrastructure. (2008). A good practice guide. United Kingdom.

Cenys, A., Rainys, D., Radvilavius, L., & Gotanin, N. (2005). Implementation of honeytoken module in dbms oracle 9ir2 enterprise edition for internal malicious activity detection. *IEEE Computer Society's TC on Security and Privacy*, 1-13.

Chen, Y., Nyemba, S., & Malin, B. (2012). Detecting anomalous insiders in collaborative information systems. *IEEE Transactions on Dependable and Secure Computing*, 9(3), 332-344.

CICA, A. (1999). Continuous Auditing: Research Report. *Toronto, Canada*.

Chiu, V., Liu, Q., & Vasarhelyi, M. A. (2018). The Development and Intellectual Structure of Continuous Auditing Research 1. In *Continuous Auditing: Theory and Application* (pp. 53-85). Emerald Publishing Limited.

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice*, 4, 225-256.

Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice*, 19, 91-150.

Clarke, R. V. G. (Ed.). (1997). *Situational crime prevention.* Monsey, NY: Criminal Justice Press. pp. 53-70.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice*, 6, 147-185.

Clarke, R. V., & Eck, J. E. (2005). *Crime analysis for problem solvers*. Washington, DC: Center for Problem-Oriented Policing.

Claycomb, W. R., & Nicoll, A. (2012, July). Insider threats to cloud computing: Directions for new research challenges. In *Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual* (pp. 387-394). IEEE.

Cleveland, F. M. (2008, July). Cyber security issues for advanced metering infrastructure (AMI). In *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008. pp. 1-5. IEEE.

Claycomb, W. R., & Nicoll, A. (2012, July). Insider threats to cloud computing: Directions for new research challenges. *In Computer Software and Applications Conference (COMPSAC)*, 2012 IEEE 36th Annual (pp. 387-394). IEEE.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 588-608.

Cole, R., Purao, S., Rossi, M., & Sein, M. (2005). Being proactive: Where action research meets design research. ICIS 2005 Proceedings International Conference on Information Systems Association for Information Systems. AIS Electronic Library (AISeL).

Coles-Kemp, L., & Theoharidou, M. (2010). Insider threat and information security management. *Insider Threats in Cyber Security*, 45-71. Springer US.

Coppola, P., Della Mea, V., Di Gaspero, L., Menegon, D., Mischis, D., Mizzaro, S., Scagnetti, I. & Vassena, L. (2010). The context-aware browser. *Intelligent Systems*, 25(1), 38-47. IEEE.

Cornish, D., & Clarke, R. (1986). Situational prevention, displacement of crime and rational choice theory. *Situational Crime Prevention: From Theory into Practice*, 1-16.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, 16, 41-96.

Cressey, D. R. (1953). *A study in the social psychology of embezzlement: Other people's money*. Glencoe, IL: Free Press.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98.

De Aquino, C. E. M., Da Silva, W. L., & Vasarhelyi, M. A. (2008). Moving toward continuous auditing: establishing audit priority areas can lead to a more effective continuous audit process. *Internal Auditor*, *65*(4), 27-30.

De Cremer, D. (2006). Unfair treatment and revenge taking: The roles of collective identification and feelings of disappointment. Group Dynamics: Theory, Research, and Practice, 10(3), 220.

Dey, A. K. (2001). Understanding and using context. *Personal and ubiquitous computing*, *5*(1), 4-7.

Dhillon, G., & Moores, S. (2001). Computer crimes: Theorizing about the enemy within. *Computers & Security*, 20(8), 715-723.

Dimkov, T., Pieters, W., & Hartel, P. H. (2009). *Portunes: generating attack scenarios by finding inconsistencies between security policies in the physical, digital and social domain*. (CTIT Technical Report Series; No. TR-CTIT-09-15). Enschede: Distributed and Embedded Security (DIES).

Dimkov, T., Pieters, W., & Hartel, P. (2010, March). Portunes: Representing attack scenarios spanning through the physical, digital and social domain. In *Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security*, 112-129. Berlin Heidelberg: Springer.

Dinges, D. F., Venkataraman, S., McGlinchey, E. L., & Metaxas, D. N. (2007). Monitoring of facial stress during space flight: Optical computer recognition combining discriminative and generative methods. *Acta Astronautica*, 60(4), 341-350.

Dobre, C., Manea, F., Cristea, V. (2011). CAPIM: A context-aware platform using integrated mobile services. In *Intelligent Computer Communication and Processing (ICCP)*, 2011. IEEE International Conference. pp. 533-540. IEEE.

Dowland, P. S., Furnell, S. M., & Papadaki, M. (2002). Keystroke analysis as a method of advanced user authentication and response. In *Security in the Information Society*, 215-226. Springer US.

Eekels, J., & Roozenburg, N. F. (1991). A methodological comparison of the structures of scientific research and engineering design: their similarities and differences. *Design Studies*, 12(4), 197-203.

Eivazi, K. (2011). Computer use monitoring and privacy at work. *Computer Law & Security Review*, 27(5), 516-523.

El Emam, K., & Dankar, F. K. (2008). Protecting privacy using k-anonymity. *Journal of the American Medical Informatics Association*, 15(5), 627-637.

El Emam, K., Dankar, F.K., Issa, R., Jonker, E., Amyot, D., Cogo, E., Corriveau, J.P., Walker, M., Chowdhury, S., Vaillancourt, R. and Roffey, T. (2009). A globally optimal k-anonymity method for the de-identification of health data. *Journal of the American Medical Informatics Association*, 16(5), 670-682.

Elmrabit, N., Yang, S. H., & Yang, L. (2015, September). Insider threats in information security categories and approaches. *Automation and Computing (ICAC).* Presented at the 21st International Conference on Automation and Computing: Automation, Computing and Manufacturing for New Economic Growth, (ICAC), Glasgow, 11-12th Sep 2015. pp. 1-6.

Evans, G. E., & Simkin, M. G. (1989). What best predicts computer proficiency? *Communications of the ACM*, 32(11), 1322-1327.

Fagade, T., Spyridopoulos, T., Albishry, N., & Tryfonas, T. (2017, July). System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 309-321). Springer, Cham.

Fagade, T., & Tryfonas, T. (2016, July). Security by compliance? A study of insider threat implications for Nigerian banks. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 128-139). Springer, Cham.

Fazekas, C. P. (2004). 1984 is still fiction: Electronic monitoring in the workplace and US privacy law. *Duke Law & Technology Review*, *3*(1), 1-17.

Flynn, L., Huth, C., Trzeciak, R., & Buttles, P. (2012, October). Best practices against insider threats for all nations. In *Cybersecurity Summit (WCS), 2012 Third Worldwide* (pp. 1-8). IEEE.

Ge, X., & Zhu, J. (2011). Privacy-preserving data mining. New Fundamental Technologies in Data Mining. InTech.

Georgiadis, C. K., Mavridis, I., Pangalos, G., & Thomas, R. K. (2001, May). *Flexible team-based access control using contexts*. Proceedings of the sixth ACM symposium on Access control models and technologies (pp. 21-27). ACM.

Gkoulalas-Divanis, A., & Loukides, G. (2013). Overview of patient data anonymization. *Anonymization of Electronic Medical Records to Support Clinical Analysis*, 9-30. Springer New York.

Goldberger, L., & Breznitz, S. (Eds.). (2010). *Handbook of stress*. Simon and Schuster.

Gregor, S. (2002). Design theory in information systems. *Australasian Journal of Information Systems*, 10(1).

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, 8(5), 312.

Grigori, D., Casati, F., Castellanos, M., Dayal, U., Sayal, M., & Shan, M. C. (2004). Business process intelligence. *Computers in industry*, *53*(3), 321-343.

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. *Insider Threats in Cyber Security*, 85-113. Springer US.

Greitzer, F. L., Frincke, D., & Zabriskie, M. (2012). Social/ethical issues in predictive insider threat monitoring. In *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1100-1129). IGI Global.

Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behaviour to anticipate insider attacks. *Journal of Strategic Security*, *4*(2), 25.

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., & Ferryman, T. (2013). Psychosocial modeling of insider threat risk based on behavioural and word use analysis. *e-Service Journal*, 9(1), 106-138.

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. (2012, January). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2392-2401). IEEE

Gritzalis, D., Stavrou, V., Kandias, M., & Stergiopoulos, G. (2014, March). Insider threat: enhancing BPM through social media. In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on* (pp. 1-6). IEEE.

Hansen, S. E., & Atkins, E. T. (1993, November). Automated System Monitoring and Notification with Swatch. In *LISA* (Vol. 93, pp. 145-152).

Hansen, J. V., & Hill, N. C. (1989). Control and audit of electronic data interchange. *MIS Quarterly*, 403-413.

Hausawi, Y. M. (2016, July). Current trend of end-users' behaviours towards security mechanisms. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 140-151). Springer, Cham.

Hempel, C. G. (1966). Philosophy of natural science. .New Jersey, U.S.A. Prentice-Hall.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75-105.

Hills, M., & Anjali, A. (2017). A human factors contribution to countering insider threats: Practical prospects from a novel approach to warning and avoiding. *Security Journal*, *30*(1), 142-152.

Hinde, S. (2003). The law, cybercrime, risk assessment and cyber protection. *Computers & Security*, *22*(2), 90-95

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, Mass: Ballinger Pub. Co.

Homel, R., & Clarke, R. (1997). A Revised Classification of Situational Crime Prevention Techniques. In *Crime Prevention at a Crossroads* (pp. 17–27). Cincinnati, OH: Anderson.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. *Security Journal*, *4*(1), 2-12.

Hori, Y., Nishide, T., & Sakurai, K. (2011, November). Towards countermeasure of insider threat in network security. In *Intelligent Networking and Collaborative Systems (INCoS), 2011 Third International Conference on* (pp. 634-636). IEEE.

Hoyer, S., Zakhariya, H., Sandner, T., & Breitner, M. H. (2012, January). Fraud prediction and the human factor: An approach to include human behaviour in an automated fraud audit. *System Science (HICSS)*. 45th Hawaii International Conference. pp. 2382-2391. IEEE.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviours and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282-300.

Hu, J., & Weaver, A. C. (2004, August). A dynamic, context-aware security infrastructure for distributed healthcare applications. In *Proceedings of the first workshop on pervasive privacy security, privacy, and trust* (pp. 1-8).

Huff, S. L., Munro, M. C., & Marcolin, B. (1992, May). *Modelling and measuring end user sophistication.* Proceedings of the 1992 ACM SIGCPR Conference on Computer Personnel Research. pp. 1-10. ACM.

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats - An overview of definitions and mitigation techniques. *JoWUA*, 2(1), 4-27.

Huth, C. L. (2013). The insider threat and employee privacy: An overview of recent case law. *Computer Law & Security Review*, *29*(4), 368-381.

IBM. 2015. Cyber Security Intelligence Index. [online]. Available at: https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf (Accessed: 2 February 2017).

Iivari, J. (2007). A paradigmatic analysis of information systems as a design science. *Scandinavian Journal of Information Systems*, 19(2), 5.

Iivari, J., & Venable, J. (2009, June). Action research and design science research-Seemingly similar but decisively dissimilar. In ECIS (pp. 1642-1653).

Jimison, H., Pavel, M., McKanna, J., & Pavel, J. (2004). Unobtrusive monitoring of computer interactions to detect cognitive status in elders. IEEE Transactions on Information Technology in Biomedicine, 8(3), 248-252.

Jimison, H., Jessey, N., McKanna, J., Zitzelberger, T., & Kaye, J. (2006, April). Monitoring computer interactions to detect early cognitive impairment in elders. In Distributed Diagnosis and Home Healthcare, 2006. D2H2. 1st Transdisciplinary Conference on (pp. 75-78). IEEE.

Kammüller, F., & Probst, C. W. (2013, May). Invalidating policies using structural information. In *Security and Privacy Workshops (SPW), 2013 IEEE* (pp. 76-81). IEEE.

Kammüller, F., & Probst, C. W. (2014, May). Combining generated data models with formal invalidation for insider threat analysis. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 229-235). IEEE.

Kammüller, F., & Probst, C. W. (2017). Modeling and verification of insider threats using logical analysis. *IEEE systems journal*, *11*(2), 534-545.

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., & Gritzalis, D. (2010, August). *An insider threat prediction model*. International Conference on Trust, Privacy and Security in Digital Business. pp. 26-37. Berlin Heidelberg: Springer.

Kandias, M., Stavrou, V., Bozovic, N., Mitrou, L., & Gritzalis, D. (2013, December). Can we trust this user? Predicting insider's attitude via YouTube usage profiling. In *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)* (pp. 347-354). IEEE.

Kassem, R., & Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences*, 3(3), 191.

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., & Rogers, S. (2005). *Insider threat study: Computer system sabotage in critical infrastructure sectors*. US Secret Service and CERT Coordination Center/SEI.

Khanna, P., & Sasikumar, M. (2010). Recognising emotions from keyboard stroke pattern. *International Journal of Computer Applications*, 11(9), 1-5.

Klein, H. K. (2003). Crisis in the IS field? A critical reflection on the state of the discipline. *Journal of the Association for Information Systems*, 4(1), 10.

Klockars, C. B. (1974). *The professional fence*. New York: Free Press.

Klompmaker, F., Nebe, K., Busch, C., & Willemsen, D. (2009). Designing context-aware user interfaces for online exercise training supervision. *Human System Interactions*, 2009. HSI'09. 2nd Conference. pp. 132-135. IEEE.

Koerber, C. P., & Neck, C. P. (2006). Religion in the workplace: Implications for financial fraud and organizational decision making. *Journal of Management, Spirituality & Religion*, 3(4), 305-318.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

Korpipaa, P., Mantyjarvi, J., Kela, J., Keranen, H., & Malm, E. J. (2003). Managing context information in mobile devices. *IEEE Pervasive Computing*, 2(3), 42-51.

Kuechler, W., & Vaishnavi, V. (2008). The emergence of design research in information systems in North America. *Journal of Design Research*, 7(1), 1-16.

Kwon, O. B. (2004). Modeling and generating context-aware agent-based applications with amended colored petri nets. *Expert Systems with Applications*, 27(4), 609-621.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information management & computer security*, *10*(2), 57-63.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707-718.

Lee, K., Yang, S., Jun, S., & Chung, M. (2007, October). Context-aware security service in RFID/USN environments using MAUT and extended GRBAC. *Digital Information Management*. ICDIM'07. 2nd International Conference, 1, 303-308. IEEE.

Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015, April). Caught in the act of an insider attack: detection and assessment of insider threat. In *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on* (pp. 1-6). IEEE.

Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2017). Automated insider threat detection system using user and role-based profile assessment. IEEE Systems Journal, 11(2), 503-512.

Levinson, A. R. (2010). Carpe diem: Privacy protection in employment act. *Akron L. Rev.*, 43, 331.

Li, W., Meng, W., & Horace, H. S. (2017). Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. Journal of Network and Computer Applications, 77, 135-145.

Lim, V. K. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behaviour*, 23(5), 675-694.

Mackevičius, J., & Giriūnas, L. (2013). Transformational research of the fraud triangle. *Ekonomika*, 92.

Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, 21(1), 62-73.

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, 24(5), 371-380.

Magklaras, G., & Furnell, S. (2010). Insider threat specification as a threat mitigation technique. In *Insider Threats in Cyber Security* (pp. 219-244). Springer, Boston, MA.

Maloof, M. A., & Stephens, G. D. (2007, September). *Elicit: A system for detecting insiders who violate need-to-know*. International Workshop on Recent Advances in Intrusion Detection. pp. 146-166. Berlin Heidelberg: Springer.

Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., Wood, B., Sibley, C., Marin, J. and Longstaff, T. (2005). Analysis and detection of malicious insiders. Massachusetts, USA. Mitre Corp Bedford.

McGrew, R. (2006, January). *Experiences with honeypot systems: Development, deployment, and analysis*. System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference, 9, 220a-220a. IEEE.

Me, G., & Spagnoletti, P. (2005). Situational crime prevention and cybercrime investigation: The online pedo-pornography case study. *Computer as a Tool*, 2005. The International Conference, 2, 1064-1067. IEEE.

Mekonnen, S., Padayachee, K., & Meshesha, M. (2015, November). A privacy preserving context-aware insider threat prediction and prevention model predicated on the components of the Fraud Diamond. *Information and Computer Technology (GOCICT).* Annual Global Online Conference. pp. 60-65. IEEE.

Memory, A., Goldberg, H. G., & Senator, T. E. (2013, June). *Context-aware insider threat detection.* Proceedings of the Workshop on Activity Context System Architectures, 44-47.

Meng, W., Li, W., Xiang, Y., & Choo, K. K. R. (2017). A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks. *Journal of Network and Computer Applications*, 78, 162-169.

Mingers, J. (2001). Combining IS research methods: Towards a pluralist methodology. *Information Systems Research*, 12(3), 240-259.

Minor, W. W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of Research in Crime and Delinquency*, 18(2), 295-318.

Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 16(4), 351-359.

Montelibano, J., & Moore, A. (2012, January). Insider threat security reference architecture. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2412-2421). IEEE.

Moore, A. D. (1998). Intangible property: Privacy, power, and information control. *American Philosophical Quarterly*, 35(4), 365-378.

Moore, A. P., Cappelli, D. M., Caron, T., Shaw, E., & Trzeciak, R. F. (2009, June). *Insider theft of intellectual property for business advantage: A preliminary model.* Proceedings of the 1st International Workshop on Managing Insider Security Threats (MIST2009). Purdue University, West Lafayette, USA.

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). The “big picture” of insider IT sabotage across US critical infrastructures. *Insider Attack and Cyber Security*, 17-52. Springer US.

Muñoz, M. A., Rodríguez, M., Favela, J., Martinez-Garcia, A. I., & González, V. M. (2003). Context-aware mobile communication in hospitals. *Computer*, *36*(9), 38-46.

Nawrocki, J. R., Jasiński, M., Olek, Ł., & Lange, B. (2005, November). *Pair programming vs. side-by-side programming*. European Conference on Software Process Improvement. pp. 28-38. Berlin Heidelberg: Springer.

Neumann, P. (1999, August). *The challenges of insider misuse.* Workshop on Research and Development Initiatives Focused on Preventing, detecting and Responding to Insider Misuse of Critical Defence Information Systems, Santa Monica, Ca. pp. 16-18.

Neumann, P. G. (2010). Combatting insider threats. *Insider Threats in Cyber Security*, 17-44. Springer US.

Nguyen, N., Reiher, P., & Kuenning, G. H. (2003, June). Detecting insider threats by monitoring system call activity. In *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society* (pp. 45-52). IEEE.

Niihara, K., Yamada, M., & Kikuchi, H. (2017, July). Sharing or Non-sharing Credentials: A Study of What Motivates People to Be Malicious Insiders. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 353-365). Springer, Cham.

Nunamaker Jr, J. F., Chen, M., & Purdin, T. D. (1990). Systems development in information systems research. *Journal of Management of Information Systems*, 7(3), 89-106.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014, May). Understanding insider threat: A framework for characterizing attacks. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 214-228). IEEE.

Omar, N. B., Din, M., & Faizal, H. (2010, December). *Fraud diamond risk indicator: An assessment of its importance and usage.* Science and Social Research (CSSR). International Conference. pp. 607-612. IEEE.

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking the "IT" in IT research - A call to theorizing the IT artefact. *Information Systems Research*, 12(2), 121-134.

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A. and Sinz, E.J. (2011). Memorandum on design-oriented information systems research. *European Journal of Information Systems*, 20(1), 7-10.

Özkul, F. U., & Pamukçu, A. (2012). Fraud detection and forensic accounting. In Emerging fraud (pp. 19-41). Springer, Berlin, Heidelberg.

Padayachee, K. (2013). A conceptual opportunity-based framework to mitigate the insider threat. *Information Security for South Africa*, 1-8. IEEE.

Padayachee, K. (2015a). An insider threat neutralisation mitigation model predicated on cognitive dissonance (ITNMCD). *South African Computer Journal*, 56(1), 50-79.

Padayachee, K. (2015b). A framework of opportunity-reducing techniques to mitigate the insider threat. *ISSA*, 1-8.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information* (pp. I-XV). New York: Wiley.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006, February). *The design science research process: A model for producing and presenting information systems research*. Proceedings of the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006). pp. 83-106. ME Sharpe, Inc.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management of Information Systems*, 24(3), 45-77.

Peisert, S., & Bishop, M. (2013). Dynamic, Flexible, and Optimistic Access Control. [online]. Available at.: http://www.escholarship.org/uc/item/2rb5352d (Accesses: 20 August 2017. eScholarship, University of California.

Piquero, N. L., Tibbetts, S. G., & Blankenship, M. B. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime practice guide. *Deviant Behaviour*, 26(2), 159-188.

Posey, C., Roberts, T., Lowry, P., Bennett, B., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviours.

Prewett, J. E., & James, E. (2004, May). Listening to your cluster with LoGS. In *The Fifth LCI International Conference on Linux Clusters: TheHPC Revolution 2004*.

Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. (2008). Countering insider threats. Dagstuhl Seminar Proceedings. [online]. Available at: http://drops.dagstuhl.de/opus/volltexte/2008/1793 (Accessed: 12 January 2017).

Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. (2010). Aspects of insider threats. In *Insider Threats in Cyber Security* (pp. 1-15). Springer, Boston, MA.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention & Community Safety*, 12(2), 99-118.

Rezaee, Z. (2002). *Financial statement fraud: Prevention and detection.* Wiley & Sons.

Rikhardsson, P., & Dull, R. (2016). An exploratory study of the adoption, application and impacts of continuous auditing technologies in small businesses. *International Journal of Accounting Information Systems*, *20*, 26-37

Rogers, J. W., & Buffalo, M. D. (1974). Neutralization techniques: Toward a simplified measurement scale. *Pacific Sociological Review*, 17(3), 313-331.

Rosenberg, R. S. (1999). The workplace on the verge of the 21st century. *Journal of Business Ethics*, 22(1), 3-14.

Rossi, M., & Sein, M. (2003). *Design research workshop: A proactive research approach.* Presentation delivered at IRIS 26, August 9-12, 2003.

Ryan, N., Pascoe, J., & Morse, D. (1999). Enhanced reality fieldwork: The context-aware archaeological assistant. *Bar International Series*, 750, 269-274.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Sah, A. (2002, November). A New Architecture for Managing Enterprise Log Data. In *LISA* (Vol. 2, pp. 121-132).

Salem, M. B., & Stolfo, S. J. (2009). *Masquerade attack detection using a search-behaviour modeling approach*. Columbia University, Computer Science Department, Technical Report CUCS-027-09.

Saltzer, J. H. (1974). Protection and the control of information sharing in Multics. *Communications of the ACM*, 17(7), 388-402.

Samarati, P. (2001). Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6), 1010-1027.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2), 38-47. IEEE Computer Society,

SANS Institute (2015). Insider threats and the need for fast and directed response. [online]. Available at: https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-37447 (Accessed: 2 February 2017).

Sanzgiri, A., & Dasgupta, D. (2016, April). *Classification of insider threat detection techniques*. Proceedings of the 11th Annual Cyber and Information Security Research Conference. p. 25. ACM.

Saranya, K., Premalatha, K., & Rajasekar, S. S. (2015, February). *A survey on privacy preserving data mining.* Electronics and Communication Systems (ICECS). 2nd International Conference. pp. 1740-1744. IEEE.

Schilit, B., Adams, N., & Want, R. (1994, December). Context-aware computing applications. In *Mobile Computing Systems and Applications, 1994. WMCSA 1994. First Workshop on* (pp. 85-90). IEEE.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526-531.

Senator, T.E, Goldberg, H.G., Memory, A., Young, W.T., Rees, B., Pierce, R., Huang, D., Reardon, M., Bader, D.A., Chow, E. and Essa, I. (2013, August). *Detecting insider threats in a real corporate database of computer usage activity.* Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. pp. 1393-1401. ACM.

Sharghi, H., & Sartipi, K. (2016, June). *A user behaviour-based approach to detect the insider threat in distributed diagnostic imaging systems.* Computer-Based Medical Systems (CBMS). IEEE 29th International Symposium. pp. 300-305. IEEE.

Shaw, E. D., & Fischer, L. F. (2005). *Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders, analysis and observations* (PERS-TR-05-13). Defence Personnel Security Research Center Monterey CA.

Shaw, E. D., Post, J. M., & Ruby, K. G. (1999). Inside the mind of the insider. *Security Management*, 43(12), 34-44.

Shaw, E. D., & Stock, H. V. (2011). *Behavioural risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall.* White Paper, Symantec, Mountain View, CA.

Simon, H. A. (1996). *The sciences of the artificial*. MIT Press.

Sinclair, S., & Smith, S. W. (2008). Preventive directions for insider threat mitigation via access control. *Insider Attack and Cyber Security*, 165-194. Springer US.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 487-502.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of research in crime and delinquency*, *34*(4), 495-518.

Skousen, C. J., Smith, K. R., & Wright, C. J. (2009). Detecting and predicting financial statement fraud: The effectiveness of the fraud triangle and SAS No. 99. *Advances in Financial Economics*, 13, 53-81.

Sogbesan, A., Ibidapo, A., Zavarsky, P., Ruhl, R., & Lindskog, D. (2012, June). *Collusion threat profile analysis: Review and analysis of MERIT model.* Internet Security (WorldCIS). World Congress. pp. 212-217. IEEE.

Sordo, M., & Vaidya, S. (Eds.). (2008). *Advanced Computational Intelligence Paradigms in Healthcare-3* (Vol. 107). Springer Science & Business Media.

Spitzner, L. (2003). *Honeypots: Tracking hackers.* Vol. 1. Reading: Addison-Wesley.

Stolfo, S. J., Bellovin, S. M., Hershkop, S., Keromytis, A. D., Sinclair, S., & Smith, S. (Eds.). (2008). *Insider attack and cyber security: Beyond the hacker.* Vol. 39. Springer Science & Business Media.

Stoll, C. (1988). Stalking the wily hacker. *Communications of the ACM*, 31(5), 484-497.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS quarterly*, 441-469.

Suh, Y. A., & Yim, M. S. (2018). "High risk non-initiating insider" identification based on EEG analysis for enhancing nuclear security. *Annals of Nuclear Energy*, *113*, 308-31.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05), 557-570.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 22(6), 664-670.

Tabak, F., & Smith, W. P. (2005). Privacy and electronic monitoring in the workplace: A model of managerial cognition and relational trust development. *Employee Responsibilities and Rights Journal*, 17(3), 173-189.

Takeda, H., Veerkamp, P., & Yoshikawa, H. (1990). Modeling design process. *AI Magazine*, 11(4), 37.

Team, I. T. I. P. (2000). DoD Insider Threat Mitigation.

Ted, E., Goldberg, H. G., Memory, A., Young, W. T., Rees, B., Pierce, R., & Essa, I. (2013, August). Detecting insider threats in a real corporate database of computer usage activity. In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 1393-1401). ACM.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6), 472-484.

Thomas, M. A., & Marathe, R. R. (2012). Determining expected behaviour of fraudsters for a continuous audit system. *IIMB Management Review*, *24*(2), 79-84.SIGKDD International Conference on Knowledge Discovery and Data Mining. pp. 1393-1401. ACM.

Thompson, P. (2004, September). Weak models for insider threat detection. *Defence and Security*, 40-48. International Society for Optics and Photonics.

Tuglular, T. (2000, March). A preliminary structural approach to insider computer misuse incidents. In *1st European Anti-Malware Conference (EICAR 2000)*.

Vaishnavi, V., & Kuechler, W. (2004). Design research in information systems. [online]. Available at: http://desrist.org/desrist/ (Accessed: 18 September 2017).

Vallgårda, S. (2012). Nudge—A new and better way to improve health? *Health policy*, *104*(2), 200-203.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263-290.

Vasarhelyi, M. A., Halper, F. B., & Ezawa, K. J. (1991). The continuous process audit system: A UNIX-based auditing tool. *The EDP Auditor Journal*, *3*(3), 85-91.

Villani, M., Tappert, C., Ngo, G., Simone, J., Fort, H. S., & Cha, S. H. (2006, June). *Keystroke biometric recognition studies on long-text input under ideal and application-oriented conditions*. Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference. pp. 39-39. IEEE.

Vizer, L. M., Zhou, L., & Sears, A. (2009). Automated stress detection using keystroke and linguistic features: An exploratory study. *International Journal of Human-Computer Studies*, 67(10), 870-886.

Von Alan, R. H., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75-105.

Walker, T. (2008). Practical management of malicious insider threat - An enterprise CSIRT perspective. *Information Security Technical Report*, 13(4), 225-234.

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an information system design theory for vigilant EIS. *Information Systems Research*, 3(1), 36-59.

Wang, W. (1999, February). *Team- and role-based organizational context and access control for cooperative hypermedia environments.* Proceedings of the 10th ACM Conference on Hypertext and Hypermedia: Returning to our Diverse Roots. pp. 37-46. ACM.

Wang, H., Yang, G., Liu, S., & Li, X. (2011, October). Research of Insider Threat Based on Bayesian Learning Theory. In Computational and Information Sciences (ICCIS), 2011 International Conference on (pp. 431-433). IEEE.

Watanabe, T., Yamada, K., & Nagatou, N. (2003, May). *Towards a specification scheme for context-aware security policies for networked appliances.* Software Technologies for Future Embedded Systems, 2003. IEEE Workshop. pp. 65-68. IEEE.

Weber, R. (1987). Toward a theory of artefacts: a paradigmatic base for information systems research. *Journal of Information Systems*, 1(2), 3-19.

Weiland, R. M., Moore, A. P., Cappelli, D. M., Trzeciak, R. F., & Spooner, D. (2010). Spotlight on: Insider threat from trusted business partners. CERT Program, Feb.

Wells, J. T. (2008). *Principles of fraud examination*. Hoboken, NJ: Wiley & Sons. pp. 277-290.

Willison, R. (2004, January). Understanding the offender/environment dynamic for computer crimes: Assessing the feasibility of applying criminological theory to the IS security context. In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on* (pp. 10-pp). IEEE.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and organization*, *16*(4), 304-324.

Willison, R., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through situational crime prevention. *Communications of the ACM*, 52(9), 133-137.

Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38.

Wood, B. (2000). An insider threat model for adversary simulation. SRI International, Research on Mitigating the Insider Threat to Information Systems, 2, 1-3.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behaviour*, *24*(6), 2799-2816.

Wullems, C., Looi, M., & Clark, A. (2004, March). Towards context-aware security: An authorization architecture for intranet environments. In Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on (pp. 132-137). IEEE.

Yang, X., Ren, X., Yang, S., & McCann, J. (2015). A novel temporal perturbation based privacy-preserving scheme for real-time monitoring systems. *Computer Networks*, 88, 72-88.

Yayla, A. A. (2011, October). Controlling insider threats with information security policies. Proceedings of 19th European Conference on Information Systems: ECIS. vol. 9, pp. 242–57.

Yu, T., Fayaz, S. K., Collins, M., Sekar, V., & Seshan, S. (2017). PSI: Precise security instrumentation for enterprise networks. In *Proceedings of the 24th Network and Distributed System Security Symposium (NDSS'17)*.

Zhang, R., Chen, X., Shi, J., Xu, F., & Pu, Y. (2014, September). *Detecting insider threat based on document access behaviour analysis*. Asia-Pacific Web Conference. pp. 376-387. Springer International Publishing.

APPENDICES

APPENDIX A: Survey Questionnaire for expert review for first iteration

Dear Participants,

Thank you so much for your willingness to complete this questionnaire. This research is being conducted by Solomon Mekonnen Tekle [49026526] of University of South Africa (UNISA) in order to comply with the requirements of his studies for the degree, PHD in Information Systems. This questionnaire is designed to gather feedback from a selected panel of insider threat experts on a model designated: A Privacy-Preserving Context-Aware Insider Threat Prevention and Prediction model. Please read the description of the model https://sites.google.com/site/citppmodel/ . Please also view the Presentation video of the model and the Proof-of-concept-video which is available online at https://sites.google.com/site/citppmodel/. You are kindly requested to respond frankly and accurately based on your understanding of the proposed model.

PART I: VALUE JUDGEMENTS

Consider the following statements and indicate whether you agree or disagree with the statement. You may support your response with a comment.

SECTION A: GENERAL EXPLORATION OF THE MODEL CONCEPT

S1: The model concept could easily be translated into an implementable product.
☐Agree
☐Disagree

Comments:

S2: The proposed model helps organizations to detect and prevent the insider threat.
☐Agree
☐Disagree

Comments:

S3: There are assumptions or steps in the model that are unreasonable.
☐Agree
☐Disagree

Comments:

S4: The proposed model can be used as a framework to aid organizations in information system security investment or development decision making processes to address the insider threat problem.
□Agree
□Disagree

Comments:

S5: The model concept can be integrated into existing systems.
□Agree
□Disagree

Comments:

S6: This model will be scalable in a real-world-context.
□Agree
□Disagree

Comments:

S7: There are NO conceivable environments in which this product concept will be applicable.
□Agree
□Disagree

Comments:

SECTION B: MOTIVE

S8: Detection of the pressures (e.g. anger, frustration or despair due to organisational factors such as denial of salary increases or personal problems) that would motivate insiders to commit maleficence is an effective means of insider threat mitigation.
□Agree
□Disagree

Comments:

S9: The emotional state of insiders (i.e. stress levels) could be predicted based on keyboard-stroke information such as change in typing speed, duration of a keystroke and the rate of mistakes.
□Agree
□Disagree

Comments:

S10: Change in resource usage behaviour (like search behaviour and download behaviour) is a viable indicator of malicious intentions.
□Agree
□Disagree

Comments:

SECTION C: OPPORTUNITY

S11: Understanding the opportunities (e.g. weak access controls) that an insider may use to launch an attack will help in minimizing the risk of cybercrime.
□Agree
□Disagree

Comments:

S12: Deploying honeytokens (i.e. a deception trap to lure insiders) by means of extraneous links, fake information on a database etc is an effective technique to identify future threats.
□Agree
□Disagree

Comments:

S13: The level of access (i.e. system role) granted to an insider (i.e. administrator, advanced, novice) could be a means of identifying insiders who may be future threats to an organization's IT infrastructure.
□Agree
□Disagree

Comments:

SECTION D: CAPABILITY

S14: The capability of a user in using the information systems of the organization (i.e. user sophistication) could be a factor for insider threat mitigation as users need to be capable of exploiting the organization's IT infrastructure in order to commit a cybercrime.
□Agree
□Disagree

Comments:

S15: The number of errors and warning messages generated by the user while using an organization's IT infrastructure could be used one of the indicators to assess skill levels of the insiders.
□Agree
□Disagree

Comments:

S16: User profiling to determine the sophistication level (i.e. capability) of insiders could be achieved by means of an examination to evaluate the knowledge of insiders with respect to computer usage (in terms of operating systems in use, techniques implemented, familiarization with specific technologies, etc).
□Agree
□Disagree

Comments:

S17: The capability of insiders could be verified based on the types of application they use and the level of computational resource usage consumed.
□Agree
□Disagree

Comments:

SECTION E: RATIONALIZATION

S18: Understanding of rationalization techniques which insiders may use to justify their crime could be used to design a neutralization mitigation strategy to circumvent any excuse for committing a crime in future.
□Agree
□Disagree

Comments:

NB: Examples of rationalizations include: denial of responsibility (i.e. placing the blame on an alternative source or circumstance); denial of injury (i.e. justifying their malicious act as it does not harm organizational property or other individuals); denial of the victim (i.e. the deviant act can be justified in the belief that the victim deserved whatever happened); condemnation of the condemners (i.e. criticizing those who condemn them in an attempt to shift the blame) and appeal to higher loyalties (i.e. justifying their criminal behaviour as being for the greater good).

S19: Posting instructions (e.g. e-mail disclaimers), a technique used by Situational Crime Prevention (SCP), could be used to remove excuses for a crime and mitigate the insider risk.
□Agree
□Disagree

Comments:

S20: Alerting conscience (e.g. via a code of ethics), which is one of the SCP techniques, could be used to remove excuses for a crime and mitigate the insider risk.
□Agree
□Disagree

Comments:

S21: Assisting compliance (e.g. hacker challenges), which is one of the SCP techniques, could be used to remove excuses for a crime and mitigate the insider risk.
□Agree
□Disagree

Comments:

S22: Setting rules (i.e. policy) that explicitly invalidate any potential defences (i.e. excuses) for cybercrime may be a useful mitigation strategy. This also implies resetting the rules based on new justifications for cybercrime.
□Agree

□Disagree

Comments:

SECTION F: PRIVACY PRESERVING

S23: Insider threat prevention and detection strategies should not infringe upon the privacy of insiders.
□Agree
□Disagree

Comments:

S24: Collecting meta-data only, such as search behaviour, file access, keystrokes and linguistic features without collecting the content of employees' communication could help to balance privacy issues associated with insider threat detection.
□Agree
□Disagree

Comments:

S25: Anonymization (i.e. removing identifiers) is an effective technique to protect individuals' identity when releasing sensitive information about potential insider threats.
□Agree
□Disagree

Comments:

SECTION G: CONTEXT ANALYSIS

S26: Understanding the context of an insider by considering the elements of usage behaviour, stress levels and the rate of error and warning messages generated is a useful mechanism towards mitigating the insider threat.

□Agree
□Disagree

Comments:

PART II: IN-DEPTH QUESTIONNAIRE

2.1 Abstraction: Does the model concept help to solve the insider threat problem in general?

Comments:

2.2 Originality: Does the model concept contribute to the advancement of the body of knowledge in information security?

Comments:

2.3 Justification: Is the model concept justified in a comprehensible manner?

Comments:

2.4 Benefit: Does the model concept yield benefit either immediately or in the future for information security?

Comments:

2.5. Any possible recommendations for improvement?

Comments:

Thank you for participation!

APPENDIX B: Survey Questionnaire for expert review for second iteration

Dear Participants,

Thank you very much for providing your expert feedback on A Privacy-Preserving Context-Aware Insider Threat Prevention and Prediction model. We have refined the model based on your constructive feedback and the model is presented for review for second iteration. This research is being conducted by Solomon Mekonnen Tekle [49026526] of University of South Africa (UNISA) in order to comply with the requirements of his studies for the degree, PHD in Information Systems. This questionnaire is designed to gather feedback from a selected panel of insider threat experts on a model designated: A Privacy-Preserving Context-Aware Insider Threat Prevention and Prediction model. Please read the updated description of the model https://sites.google.com/site/citppmodel/.Please also view the updated Presentation video of the model and the Proof-of-concept-video which is available online at https://sites.google.com/site/citppmodel/. You are kindly requested to respond frankly and accurately based on your understanding of the proposed model.

PART I: VALUE JUDGEMENTS

Consider the following statements and indicate whether you agree or disagree with the statement. You may support your response with a comment.

SECTION A: GENERAL EXPLORATION OF THE MODEL CONCEPT

S1: The model concept could easily be translated into an implementable product.
☐Agree
☐Disagree

Comments:

S2: The proposed model helps organizations to detect and prevent the insider threat.
☐Agree
☐Disagree

Comments:

S3: There are assumptions or steps in the model that are unreasonable.
☐Agree
☐Disagree

Comments:

S4: The proposed model can be used as a framework to aid organizations in information system security investment or development decision making processes to address the insider threat problem.
□Agree
□Disagree

Comments:

S5: The model concept can be integrated into existing systems.
□Agree
□Disagree

Comments:

S6: This model will be scalable in a real-world-context.
□Agree
□Disagree

Comments:

S7: There are NO conceivable environments in which this product concept will be applicable.
□Agree
□Disagree

Comments:

SECTION B: MOTIVE

S8: Detection of the pressures with learning new behaviour (e.g. anger, frustration or despair due to organisational factors such as denial of salary increases or personal problems) that would motivate insiders to commit maleficence is an effective means of insider threat mitigation.
□Agree
□Disagree

Comments:

S9: The emotional state of insiders with learning new behaviour (i.e. stress levels) could be predicted based on keyboard-stroke information such as change in typing speed, duration of a keystroke and the rate of mistakes.
□Agree
□Disagree

Comments:

S10: Change in resource usage behaviour with learning new behaviour (like search behaviour and download behaviour) is a viable indicator of malicious intentions.
□Agree
□Disagree

Comments:

SECTION C: OPPORTUNITY

S11: Understanding the opportunities (e.g. weak access controls) that an insider may use to launch an attack will help in minimizing the risk of cybercrime.
□Agree
□Disagree

Comments:

S12: Deploying honeytokens (i.e. a deception trap to lure insiders) by means of extraneous links, fake information on a database etc is an effective technique to identify future threats.
□Agree
□Disagree

Comments:

S13: The level of access (i.e. system role) granted to an insider (i.e. administrator, advanced, novice) could be a means of identifying insiders who may be future threats to an organization's IT infrastructure.
□Agree
□Disagree

Comments:

SECTION D: CAPABILITY

S14: The capability of a user in using the information systems of the organization (i.e. user sophistication) could be a factor for insider threat mitigation as users need to be capable of exploiting the organization's IT infrastructure in order to commit a cybercrime.
□Agree
□Disagree

Comments:

S15: The number of errors and warning messages generated by the user while using an organization's IT infrastructure to which he/she familiar with could be used one of the indicators to assess skill levels of the insiders including other variables like amount of errors and frequency in short period of time

□Agree
□Disagree

Comments:

S16: User profiling to determine the sophistication level (i.e. capability) of insiders could be achieved by means of an examination to evaluate the knowledge of insiders with respect to computer usage (in terms of operating systems in use, techniques implemented, familiarization with specific technologies, etc) with learning new behaviour .
□Agree
□Disagree

Comments:

S17: The capability of insiders could be verified based on the types of application they use and the level of computational resource usage consumed.

□Agree
□Disagree

Comments:

SECTION E: RATIONALIZATION

S18: Understanding of rationalization techniques which insiders may use to justify their crime could be used to design a neutralization mitigation strategy to circumvent any excuse for committing a crime in future.
□Agree
□Disagree

Comments:

NB: Examples of rationalizations include: denial of responsibility (i.e. placing the blame on an alternative source or circumstance); denial of injury (i.e. justifying their malicious act as it does not harm organizational property or other individuals); denial of the victim (i.e. the deviant act can be justified in the belief that the victim deserved whatever happened); condemnation of the condemners (i.e. criticizing those who condemn them in an attempt to shift the blame) and appeal to higher loyalties (i.e. justifying their criminal behaviour as being for the greater good).

S19: Posting instructions (e.g. e-mail disclaimers), a technique used by Situational Crime Prevention (SCP), could be used to remove excuses for a crime and mitigate the insider risk.
□Agree
□Disagree

Comments:

S20: Alerting conscience (e.g. via a code of ethics), which is one of the SCP techniques, could be used to remove excuses for a crime and mitigate the insider risk.
□Agree
□Disagree

Comments:

S21: Assisting compliance (e.g. hacker challenges), which is one of the SCP techniques, could be used to remove excuses for a crime and mitigate the insider risk.
□Agree
□Disagree

Comments:

S22: Setting rules (i.e. policy) that explicitly invalidate any potential defences (i.e. excuses) for cybercrime may be a useful mitigation strategy. This also implies resetting the rules based on new justifications for cybercrime.
□Agree
□Disagree

Comments:

SECTION F: PRIVACY PRESERVING

S23: Insider threat prevention and detection strategies should not infringe upon the privacy of insiders.
□Agree
□Disagree

Comments:

S24: Collecting meta-data only, such as search behaviour, file access, keystrokes and linguistic features without collecting the content of employees' communication could help to balance privacy issues associated with insider threat detection.
□Agree
□Disagree

Comments:

S25: Anonymization (i.e. removing identifiers) is an effective technique to protect individuals' identity when releasing sensitive information about potential insider threats.
□Agree
□Disagree

Comments:

SECTION G: CONTEXT ANALYSIS

S26: Understanding the context of an insider by considering the elements of usage behaviour, stress levels and the rate of error and warning messages generated is a useful mechanism towards mitigating the insider threat.

□Agree
□Disagree

Comments:

PART II: IN-DEPTH QUESTIONNAIRE

2.1 Abstraction: Does the model concept help to solve the insider threat problem in general?

Comments:

2.2 Originality: Does the model concept contribute to the advancement of the body of knowledge in information security?

Comments:

2.3 Justification: Is the model concept justified in a comprehensible manner?

Comments:

2.4 Benefit: Does the model concept yield benefit either immediately or in the future for information security?

Comments:

2.5. Any possible recommendations for improvement?

Comments:

Thank you for participation!

APPENDIX C: Code for prototype version I

```
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
     pageEncoding="ISO-8859-1"%>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>CheckerMenu</title>
<script type="text/javascript"
src="../javascripts/jquery.min.js"></script>
<script type="text/javascript"
src="../javascripts/animatedcollapse.js"></script>
<script type="text/javascript" language="javascript"
     src="../javascripts/jquery.js"></script>
<link type="text/css" rel="stylesheet" href="../css/styles.css"
/>
<script type="text/javascript">
     $(document).ready(
                function() {
                     //slides the element with class "menu_body"
when paragraph with class "menu_head" is clicked
                     $("#secondary p.menu_head").click(
                                function() {
                                     $(this).css({
                                          backgroundImage :
"url(image/down.png)"

     }).next("div.menu_body").slideToggle(300).siblings(

     "div.menu_body").slideUp("slow");
                                     $(this).siblings().css({
                                          backgroundImage :
"url(image/left.png)"
                                     });
                                });
                });
</script>
</head>
<%
     if (request.getSession().getAttribute("loginName") == null)
{


     request.getRequestDispatcher("sessionExpaire.jsp").forward(
                     request, response);

     } else {
```

```
%>

<body bgcolor="#F8FAFF">

      <div id="bd">
            <div id="secondary" class="menu_list">
                  <p class="menu_head">Authorizer</p>
                  <div class="menu_body">
                        <a href="authorizevehiclerecords.jsp"
target="content" target="content">authorize vehicle</a>
                        <a href="authorizeitempurchasedrecords.jsp"
target="content" target="content">authorize item purchased</a>
                        <a href="authorizeitemrequestedrecords.jsp"
target="content" target="content">authorize item requested</a>
                        <a
href="authorizeitemdistributedrecords.jsp" target="content"
target="content">authorize item distributed</a>
                        <a href="listofatriskinsiders.jsp"
target="content" target="content">Anonymized list of suspected
insiders</a>
                        <a href="behaviourofinsiders.jsp"
target="content" target="content">Anonymized report on Behaviour
insiders</a>

                  </div>
            </div>
      </div>
</body>
<%
      }
%>
</html>

<%@ page language="java" contentType="text/html; charset=ISO-
8859-1" %>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>Display List of At-risk Insiders</title>
<link rel="stylesheet" href="../css/structure.css"
type="text/css" />
<link rel="stylesheet" href="../css/form.css" type="text/css" />
<link rel="stylesheet" href="../css/theme.css" type="text/css" />
<link rel="stylesheet" href="../css/viewTable.css"
type="text/css"></link>

<script type="text/javascript">
      function altRows(id) {
            if (document.getElementsByTagName) {
```

```
                var table = document.getElementById(id);
                var rows = table.getElementsByTagName("tr");

                for (i = 0; i < rows.length; i++) {
                     if (i % 2 == 0) {
                          rows[i].className = "evenrowcolor";
                     } else {
                          rows[i].className = "oddrowcolor";
                     }
                }
           }
     }
     window.onload = function() {
          altRows('alternatecolor');
     }
</script>
</head>
<body>
<form name=myform>
<table class="report" id="alternatecolor" align="center">
    <tr>
        <td colspan="6" align="center" style="background-
color:#76AC78;color:#0000FF;"><b>Anonymized report on behaviour
of Insiders</b></td>
    </tr>
    <tr style="background-color: #efefef;">
        <th><b>code</b></th>
        <th><b>Motive(out of 3)</b></th>
        <th><b>Capability(out of 3)</b></th>
        <th><b>Threat Level</b></th>
        <th><b>Honeytocken attack?</b></th>
        <th><b>Rationalizations used</b></th>
    </tr>
 <tr><td>A</td><td>2 (Medium)</td><td>3
(High)</td><td>Dangerous</td><td>Yes</td><td>This will not harm
any one (Denial of enquiry) and It was an urgent and important
task for my job (Appeal to higher authorities)</td></tr>
 <tr><td>B</td><td>2 (Medium) </td><td>2 (Medium)</td><td>Medium
Risk</td><td>No</td></tr>
 <tr><td>C<td>3 (High)</td><td>2 (Medium)
</td><td>Dangerous</td><td>Yes</td><td>I have been loyal to the
organization and the access should have been authorized (The
metaphor of the ledger)</td></tr>
</table>
</form>
</body></html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1" %>
<!DOCTYPE html>
<html>
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>Display List of At-risk Insiders</title>
<link rel="stylesheet" href="../css/structure.css"
type="text/css" />
<link rel="stylesheet" href="../css/form.css" type="text/css" />
<link rel="stylesheet" href="../css/theme.css" type="text/css" />
<link rel="stylesheet" href="../css/viewTable.css"
type="text/css"></link>

<script type="text/javascript">
     function altRows(id) {
          if (document.getElementsByTagName) {

               var table = document.getElementById(id);
               var rows = table.getElementsByTagName("tr");

               for (i = 0; i < rows.length; i++) {
                    if (i % 2 == 0) {
                         rows[i].className = "evenrowcolor";
                    } else {
                         rows[i].className = "oddrowcolor";
                    }
               }
          }
     }
     window.onload = function() {
          altRows('alternatecolor');
     }
</script>
</head>
<body>
<form name=myform>
<table class="report" id="alternatecolor" align="center">
    <tr>
        <td colspan="5" align="center" style="background-
color:#76AC78;color:#0000FF;"><b>Anonymized List of At-risk
Insiders</b></td>
    </tr>
    <tr style="background-color: #efefef;">
        <th><b>code</b></th>
        <th><b>Motive(out of 3)</b></th>
        <th><b>Capability(out of 3)</b></th>
        <th><b>Threat Level</b></th>
    </tr>
 <tr><td>A</td><td>2 (Medium)</td><td>3
(High)</td><td>Dangerous</td></tr>
 <tr><td>B</td><td>2 (Medium) </td><td>2 (Medium)</td><td>Medium
Risk</td></tr>
 <tr><td>C<td>3 (High)</td><td>2 (Medium)
</td><td>Dangerous</td></tr>
```

```
 <tr><td><input type="button" name="Submit" value="Facilitate
Opportunity" onClick="if(confirm('Are you sure about facilitating
the honey token?'))
alert('Honey Token Facilitated!');"></td></tr>
</table>
</form>
</body></html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
     pageEncoding="ISO-8859-1"%>
    <% String
loginName=(String)session.getAttribute("sloginName");
    String password=(String)session.getAttribute("spassword");
    session.setAttribute("sloginName",loginName);
    session.setAttribute("spassword",password);%>
<!DOCTYPE html>
<html>
<%
String checkPath="";
String path="";
String errorColor="";
if (request.getAttribute("checkPath")!=null){
      checkPath=(String)request.getAttribute("checkPath");

 if (checkPath.compareToIgnoreCase("servlet")==0){

       path="./";

 }else{
       path="../";
 }
}else{
      path="../";
}
%>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<link rel="stylesheet" href=<%=path + "css/structure.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/form.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/theme.css"%>
type="text/css" />
          <title>

          </title>

     </head>
     <% if (request.getSession().getAttribute("loginName") ==
null) {
```

```
      request.getRequestDispatcher("sessionExpaire.jsp")
                  .forward(request, response);

} else {
      String message="";
      if (request.getAttribute("message")==null){
               message= "";
      }else{
             message= (String) request.getAttribute("message");
      }
      if (message.compareToIgnoreCase("Operation is
successful")==0){
            errorColor="Blue";
      }else{
            errorColor="Red";
      }
      String []reason=(String []) request.getAttribute("reason");

      %>
      <body id="public">
      <div id="container" Style="height: 500px">
<form method="post"action="./displayinfoplicytrainingfull">
<h4>Warning</h4>
<%
for(String s:reason)
      {
      %>
      <p><%=s %></p>
      <%
      }
      %>
<p>please Visit <a
href="http://www.demopolicytraining.com">http://www.demopolicytra
ining.com</a> for more information</p>
<p>Click Ok to Continue</p><br>
<input type="submit" name="OK" value="OK">
</form>
</div>
      </body>
      <%message="";} %>
</html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
      pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>CheckerMenu</title>
```

```
<script type="text/javascript"
src="../javascripts/jquery.min.js"></script>
<script type="text/javascript"
src="../javascripts/animatedcollapse.js"></script>
<script type="text/javascript" language="javascript"
     src="../javascripts/jquery.js"></script>
<link type="text/css" rel="stylesheet" href="../css/styles.css"
/>
<script type="text/javascript">

$(document).ready(function()
{
     //slides the element with class "menu_body" when paragraph
with class "menu_head" is clicked
     $("#secondary p.menu_head").click(function()
    {

     $(this).css({backgroundImage:"url(image/down.png)"}).next("
div.menu_body").slideToggle(300).siblings("div.menu_body").slideU
p("slow");

     $(this).siblings().css({backgroundImage:"url(image/left.png
)"});
     });
});
</script>
</head>
<%
if (request.getSession().getAttribute("loginName") == null) {

     request.getRequestDispatcher("sessionExpaire.jsp")
                .forward(request, response);

} else {

%>
<body bgcolor="#F8FAFF">

     <div id="bd">
     <div id="secondary" class="menu_list">
                <p class="menu_head">Item Purchased</p>
                <div class="menu_body">
                     <a href="itempurchased.jsp"
target="content">add</a> <a
                          href="edititempurchased.jsp"
target="content">update</a> <a
                          href="displaypurchaseditem.jsp"
target="content">list</a></div>
                <p class="menu_head">Item Requested</p>
                <div class="menu_body">
                     <a href="itemrequested.jsp"
target="content">add</a> <a
```

```
                              href="edititemrequested.jsp"
target="content">update</a> <a
                              href="displayrequesteditem.jsp"
target="content">list</a></div>
                  <p class="menu_head">Item Distributed</p>
                  <div class="menu_body">
                        <a href="selectitemdistributed.jsp"
target="content">distribute item</a>
                        <!-- <a
                              href="edititemdistributed.jsp"
target="content">update</a> -->
                              <a
                              href="displaydistributeditem.jsp"
target="content">list</a></div>
                  <p class="menu_head">Item Transfered</p>
                  <div class="menu_body">
                        <a href="selecttransferitems.jsp"
target="content">Transfer item</a>
                        <a
                              href="edititemtransfered.jsp"
target="content">update</a>
                              <a
                              href="displaydistributeditem.jsp"
target="content">list</a></div>
                  <p class="menu_head">vehicle</p>
                  <div class="menu_body">
                        <a href="vehicleregistration.jsp"
target="content">add</a> <a
                              href="editvehicleregistration.jsp"
target="content">update</a> <a
                              href="vehicledisplay.jsp"
target="content">list</a></div>
                  <p class="menu_head">check item availablity</p>
                  <div class="menu_body">
                        <a href="displaycheckitemavailablity.jsp"
target="content">check item</a>
                  </div>
                  <p class="menu_head">Authorize</p>
                  <div class="menu_body">
                        <a href="list.jsp"
target="content">Authorize item</a>
                  </div>
                  </div>
</body>
<%} %>
</html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html>
<html>
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>Fixed Asset MANAGEMENT SYSTEM</title>
</head>
<%@ page import="javax.servlet.http.HttpServletResponse" %>
                      <frameset rows="70,*,40" frameborder="0"
border="0" framespacing="0">
                           <frame frameborder="2.5" name="header"
scrolling=no noresize=noresize src="../header.jsp">
                           <frameset cols="200,*" frameborder="0"
border="0" framespacing="0">
                           <frame name="menu"
src="maliciuschecker.jsp"   marginheight="3" marginwidth="18"
scrolling="no" noresize>
                           <frame name="content"
src="dbeintro.html" marginheight="0" marginwidth="0"
scrolling="auto" noresize>
                           </frameset>
                           <frame name="footer"
src="../footer.html" scrolling="no" noresize>
                           <noframes>
                           </noframes>
                           </frameset>

</html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1" %>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">

 </table>
</form>
</body></html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
     pageEncoding="ISO-8859-1"%>
    <% String
loginName=(String)session.getAttribute("sloginName");
    String password=(String)session.getAttribute("spassword");
    session.setAttribute("sloginName",loginName);
    session.setAttribute("spassword",password);%>
<!DOCTYPE html>
<html>
<%
String checkPath="";
String path="";
String errorColor="";
if (request.getAttribute("checkPath")!=null){
      checkPath=(String)request.getAttribute("checkPath");
```

```
 if (checkPath.compareToIgnoreCase("servlet")==0){

       path="./";

 }else{
       path="../";
 }
}else{
      path="../";
}
%>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<link rel="stylesheet" href=<%=path + "css/structure.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/form.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/theme.css"%>
type="text/css" />
           <title>
                Register Process or Branch
           </title>

     </head>
     <% if (request.getSession().getAttribute("loginName") ==
null) {

     request.getRequestDispatcher("sessionExpaire.jsp")
                .forward(request, response);

} else {
     String message="";
     if (request.getAttribute("message")==null){
              message= "";
     }else{
            message= (String) request.getAttribute("message");
     }
     if (message.compareToIgnoreCase("Operation is
successful")==0){
           errorColor="Blue";
     }else{
           errorColor="Red";
     }
     %>
     <body id="public">
     <div id="container" Style="height: 500px">
<form method ="post"action="<%=path
+"displayinfoplicytraining"%>">
<p>You may have accessed information that was not under your
access permission</p>
```

```
<input type="checkbox" name="reason" value="Denail of
responsiblity is violating the Information security policy of the
organization">It is an error casused by the computer system<br>
<input type="checkbox" name="reason" value="Denial of inquiry is
violating the Information security policy of the organization
">This will not harm any one.<br>
<input type="checkbox" name="reason" value="Appeal to higher
authorities is violating the Information security policy of the
organization ">It was an urgent and important task for my
job.<br>
<input type="checkbox" name="reason" value="The metaphor of the
ledger is violating the Information security policy of the
organization "> I have been loyal to the organization and the
access should have been authorized.<br>
<input type="checkbox" name="reason" value="Condemnation of the
condemners is violating the Information security policy of the
organization ">The Manager was abscent at that time.<br><br><br>
<p>Click Ok to Continue</p><br><br>
<input type="submit" name="OK" value="OK">
</form>
</div>
     </body>
     <%message="";} %>
</html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
     pageEncoding="ISO-8859-1"%>
<%@ page
     import="java.util.*,java.sql.*,com.dbe.fam.datamanager.DbCo
nnection"%>
    <% String
loginName=(String)session.getAttribute("sloginName");
    String password=(String)session.getAttribute("spassword");
    session.setAttribute("sloginName",loginName);
    session.setAttribute("spassword",password);%>
<!DOCTYPE html>
<html>
<%
String checkPath="";
String path="";
String errorColor="";
if (request.getAttribute("checkPath")!=null){
      checkPath=(String)request.getAttribute("checkPath");

 if (checkPath.compareToIgnoreCase("servlet")==0){

       path="./";

 }else{
       path="../";
 }
}else{
```

```
      path="../";
}
%>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<link rel="stylesheet" href=<%=path + "css/structure.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/form.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/theme.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/viewTable.css"%>
type="text/css"></link>

<SCRIPT type="text/javascript">
        function addRow(tableID) {
 //comment
            var table = document.getElementById(tableID);

            var rowCount = table.rows.length;
            var row = table.insertRow(rowCount);

            var colCount = table.rows[0].cells.length;

            for(var i=0; i<colCount; i++) {

                var newcell = row.insertCell(i);

                newcell.innerHTML =
table.rows[0].cells[i].innerHTML;
                //alert(newcell.childNodes);
                switch(newcell.childNodes[0].type) {
                    case "text":

                            newcell.childNodes[0].value = "";
                            break;
                    case "checkbox":
                            newcell.childNodes[0].checked =
false;
                            break;
                    case "select-one":
                            newcell.childNodes[0].selectedIndex =
0;
                            break;
                }
            }
        }

        function deleteRow(tableID) {
            try {
            var table = document.getElementById(tableID);
```

```
            var rowCount = table.rows.length;

            for(var i=0; i<rowCount; i++) {
                var row = table.rows[i];
                var chkbox = row.cells[0].childNodes[0];
                if(null != chkbox && true == chkbox.checked) {
                    if(rowCount <= 1) {
                        alert("Cannot delete all the rows.");
                        break;
                    }
                    table.deleteRow(i);
                    rowCount--;
                    i--;
                }


            }
            }catch(e) {
                alert(e);
            }
        }

    </SCRIPT>
    <script type="text/javascript">
      function altRows(id) {
            if (document.getElementsByTagName) {

                  var table = document.getElementById(id);
                  var rows = table.getElementsByTagName("tr");
                  for (var i = 0; i < rows.length; i++) {
                        if (i % 2 == 0) {
                              rows[i].className = "evenrowcolor";
                        } else {
                              rows[i].className = "oddrowcolor";
                        }
                  }
            }
      }
      window.onload = function() {
            altRows('alternatecolor');
      }
</script>
            <title>
                  Display Item Purchased
            </title>

      </head>
      <% if (request.getSession().getAttribute("loginName") ==
null) {

      request.getRequestDispatcher("sessionExpaire.jsp")
                  .forward(request, response);
```

```
} else {
      String message="";
      if (request.getAttribute("message")==null){
              message= "";
      }else{
             message= (String) request.getAttribute("message");
      }
      if (message.compareToIgnoreCase("Operation is
successful")==0){
           errorColor="Blue";
      }else{
           errorColor="Red";
      }
      String ogrn="";
      String purchase_date="";
      String supplier_name = null;
      String ssize=request.getAttribute("size").toString();
      int size=Integer.parseInt(ssize);
      String item_name[]=new String[size];
      double [] unit_price=new double[size];
      int [] quantity=new int[size];
      int [] warranty_period=new int[size];
      String [] item_description=new String[size] ;
    Connection con = null;
      ResultSet rs = null;
      Statement stmt = null;
      ogrn=request.getAttribute("grn").toString();
      supplier_name=request.getAttribute("supplier_name").toStrin
g();
      purchase_date=request.getAttribute("purchase_date").toStrin
g();
      item_description=
(String[])request.getAttribute("item_description");
      item_name=(String[])request.getAttribute("item_name");
      quantity=(int[])request.getAttribute("quantity");
      warranty_period=(int[])request.getAttribute("warranty_perio
d");
      unit_price=(double[])request.getAttribute("unit_price");
      String year="";
      String month="";
      String date="";
      year=purchase_date.substring(0,4);
      month=purchase_date.substring(5,7);
      date=purchase_date.substring(8,10);
      purchase_date=date+"/"+month+"/"+year;
      %>
      <body id="public">
      <!--       <div id="container" width="800px">-->
      <div id="container"style="width:800px">
           <div style="width:800px; background-color: #66A666;
color: white" align="center">
```

```
                <h4>Display Item Purchased</h4>
            </div>
            <form action="<%=path +"authorizeitempurchased"%>"
method="post">
                 <table width="800px" border="0" align="center"
class="customers"  bgcolor= #F0FFFF  id="alternatecolor"
valign="top">
                      <tr><th>GRN :</th><td><input type="number"
name="grn" id="grn" value="<%=ogrn%>" maxlength="6" readonly
/></td></tr>
                      <tr><th>Supplier Name: </th><td>
                  <input type="text" name="supplier_name"
id="supplier_name" value="<%=supplier_name%>" width="20%"
readonly>
</TD>
</tr>
<tr><th>Purchased Date: </th><td><input type="text"
name="purchase_date" value="<%=purchase_date%>"
readonly/></td></tr>
</table>
 <table align="center"  width="800px" border="0" bgcolor= #AEDCF2
class="customers">
  <tr>
   <th align="center">Item Name</th>
   <th align="center">Item Description</th>
   <th align="center">Unit Price</th>
   <th align="center">Quantity</th>
   <th align="center">Warranty Period</th>
   </tr>
   <%
   String oitem_name="";
   for(int x=0; x<size;x++){
   %>
      <tr>
           <td ><input type="text" name="item_name"
            id="item_name" value="<%=item_name[x]%>" readonly>
        </td>
                      <td><input type="text"
name="item_description" id="item_description"
value="<%=item_description[x]%>"readonly /></td>
                      <td><div style="margin-right: 3px;"><div
style="padding-right: 3px;"><input type="number"
name="unit_price" id="unit_price" value="<%=unit_price[x]%>"
style="width:50%;"readonly/></div></div></td>
                      <td><div style="margin-right: 3px;"><div
style="padding-right: 3px;"><input type="number" name="quantity"
id="quantity"
value="<%=quantity[x]%>"style="width:50%;"readonly/></div></div><
/td>
                      <td><div style="margin-right: 3px;"><div
style="padding-right: 3px;"><input type="number"
name="warranty_period" id="warranty_period"
```

```
value="<%=warranty_period[x]%>"style="width:50%;"readonly/></div>
</div></td></tr>
                        <%} %>
      </table>
      <table align="center" width="800px" border="0"
bgcolor=#E0F5FF class="customers">
      <tr><td><input type="submit" name="authorize"
value="authorize"/></td></tr>
      <% if(message!=""){%>
                        <tr><td colspan="2"><font face="verdana"
color="<%=errorColor%>"><%=message%></font></td></tr>

                        <%} %>
      </table>
       </form>
      </div>
      </body>
      <%message="";} %>
</html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
      pageEncoding="ISO-8859-1"%>
    <% String
loginName=(String)session.getAttribute("sloginName");
    String password=(String)session.getAttribute("spassword");
    session.setAttribute("sloginName",loginName);
    session.setAttribute("spassword",password);%>
    <%@ page
import="java.util.*,java.sql.*,com.dbe.fam.datamanager.DbConnecti
on"%>
<!DOCTYPE html>
<html>
<%
String checkPath="";
String path="";
String errorColor="";
Connection con = null;
ResultSet rs = null;
Statement stmt = null;
if (request.getAttribute("checkPath")!=null){
       checkPath=(String)request.getAttribute("checkPath");

 if (checkPath.compareToIgnoreCase("servlet")==0){

        path="./";

 }else{
       path="../";
 }
}else{
       path="../";
}
```

```
%>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>Create user</title>
<link rel="stylesheet" href=<%=path + "css/structure.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/form.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/theme.css"%>
type="text/css" />
          <title>
               Register Employee
          </title>

     </head>
     <% if (request.getSession().getAttribute("loginName") ==
null) {

     request.getRequestDispatcher("sessionExpaire.jsp")
                .forward(request, response);

} else {
     String message="";
     if (request.getAttribute("message")==null){
             message= "";
     }else{
            message= (String) request.getAttribute("message");
     }
     if (message.compareToIgnoreCase("Operation is
successful")==0){
          errorColor="Blue";
     }else{
          errorColor="Red";
     }%>
     <body id="public">
     <div id="container" Style="height: 500px">
          <div style="background-color: #66A666; color: white"
align="center">
               <h4>Register Employee</h4>
          </div>
          <form method="post" action=<%=path +
"EmployeeRegistration"%>>
               <table align="center">
                    <tr><th>Employee ID: </th><td><input
type="text" name="employee_id" required pattern="^[\a-zA-z0-
9\\]+$" class="inputbox" /></td></tr>
                    <tr><th>Employee Name: </th><td><input
type="text" name="employee_name" maxlength="100" pattern="[A-Za-
z\/\s]{3,100}" required class="inputbox" /></td></tr>
                    <tr><th>Process or Branch</th>
                     <td><select name="process_name" size="1">
```

```
                                        <%DbConnection connect =
new DbConnection();
                                        con =
connect.getSingleConnection();

                                        stmt =
con.createStatement();

                                        String sqls = "SELECT
process_name from process_or_branch order by process_name";
                                        System.out.println(sqls);
                                        rs =
stmt.executeQuery(sqls);
                                        String process_name="";
                                                  %>

                                                  <%
                                                        while
(rs.next()) {

      process_name = rs.getString("process_name");

                                                  %>
                                        <option
value="<%=process_name%>"><%=process_name%></option>
                                        <%} %>

                                        </select></td>
                                        </tr>
                        <tr><td colspan="2"><font face="verdana"
color="<%=errorColor %>"><%=message %></font><td></tr>
                        <tr><th></th><td><input type="submit"
name="REGISTER" value="Register">
                        </td></tr>
                  </table>
            </form>
            </div>
      </body>
      <%message="";} %>
</html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
      pageEncoding="ISO-8859-1"%>
<%@ page
import="java.util.*,java.sql.*,com.dbe.fam.datamanager.DbConnecti
on"%>
    <% String
loginName=(String)session.getAttribute("sloginName");
    String password=(String)session.getAttribute("spassword");
    session.setAttribute("sloginName",loginName);
    session.setAttribute("spassword",password);%>
<!DOCTYPE html>
```

```
<html>
<%
String checkPath="";
String path="";
String errorColor="";
String category_name = null;
String sub_category_name = null;
String life_time=null;
Connection con = null;
ResultSet rs = null;
Statement stmt = null;
if (request.getAttribute("checkPath")!=null){
      checkPath=(String)request.getAttribute("checkPath");

 if (checkPath.compareToIgnoreCase("servlet")==0){

       path="./";

 }else{
       path="../";
 }
}else{
      path="../";
}
%>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<link rel="stylesheet" href=<%=path + "css/structure.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/form.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/theme.css"%>
type="text/css" />
           <title>
                Register Item
           </title>

     </head>
     <% if (request.getSession().getAttribute("loginName") ==
null) {

     request.getRequestDispatcher("sessionExpaire.jsp")
                .forward(request, response);

} else {
     String message="";
     if (request.getAttribute("message")==null){
             message= "";
     }else{
            message= (String) request.getAttribute("message");
     }
```

```
     if (message.compareToIgnoreCase("Operation is
successful")==0){
          errorColor="Blue";
     }else{
          errorColor="Red";
     }%>
     <body id="public">
     <div id="container" Style="height: 500px">
          <div style="background-color: #66A666; color: white"
align="center">
               <h4>Register Item</h4>
          </div>
          <form method="post" action=<%=path +
"ItemRegistration"%>>
               <table align="center">
                    <tr><th>Item Category: </th>
                <td><select name="category_name" size="1">
                                   <% DbConnection connect =
new DbConnection();
                                                        con =
connect.getSingleConnection();

                                                        stmt
= con.createStatement();


     String sqls = "SELECT category_name from item_category
order by category_name";

     System.out.println(sqls);
                                                        rs =
stmt.executeQuery(sqls);
                                                   %>

                                                   <%
                                                        while
(rs.next()) {

     category_name = rs.getString("category_name");

                                                   %>
                                   <option
value="<%=category_name%>"><%=category_name%></option>
                                   <%} %>

                                   </select></td>
                                   </tr>
                    <tr><th>Item Sub Category:</th>
                     <td><select name="sub_category_name"
size="1">
                                   <%
```

```
                                                    String sqls1 =
"SELECT sub_category_name from item_sub_category order by
sub_category_name";

     System.out.println(sqls);
                                                    rs =
stmt.executeQuery(sqls1);
                                                    %>

                                                    <%
                                                         while
(rs.next()) {

     sub_category_name = rs.getString("sub_category_name");


                                                    %>
                                               <option
value="<%=sub_category_name%>"><%=sub_category_name%></option>
                                               <%} %>

                                               </select></td>
                                               </tr>
                         <tr><th>Item Name: <th><input type="text"
name="item_name" maxlength="100" required pattern="[a-zA-
Z]{3,100}"class="inputbox" /> </th></tr>
                         <tr><th>Item ID: <th><input type="text"
name="item_id" maxlength="6" required pattern="[0-9-.]{5,6}"
class="inputbox" /> </th></tr>
                         <tr><td colspan="2"><font face="verdana"
color="<%=errorColor %>"><%=message %></font><td></tr>
                         <tr><th></th><td><input type="submit"
name="REGISTER" value="Register"></td></tr>
                    </table>
               </form>
               </div>
     </body>
     <%message="";} %>
</html>
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
     pageEncoding="ISO-8859-1"%>

<!DOCTYPE html>
<html>
<%
String checkPath="";
String path="";
String errorColor="";
if (request.getAttribute("checkPath")!=null){
       checkPath=(String)request.getAttribute("checkPath");
```

```
 if (checkPath.compareToIgnoreCase("servlet")==0){

       path="./";

 }else{
       path="../";
 }
}else{
      path="../";
}
%>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<link rel="stylesheet" href=<%=path + "css/structure.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/form.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/theme.css"%>
type="text/css" />
<link rel="stylesheet" href=<%=path + "css/viewTable.css"%>
type="text/css"></link>
<SCRIPT type="text/javascript">
        function addRow(tableID) {
 //comment
            var table = document.getElementById(tableID);

            var rowCount = table.rows.length;
            var row = table.insertRow(rowCount);

            var colCount = table.rows[0].cells.length;

            for(var i=0; i<colCount; i++) {

                var newcell = row.insertCell(i);

                newcell.innerHTML =
table.rows[0].cells[i].innerHTML;
                //alert(newcell.childNodes);
                switch(newcell.childNodes[0].type) {
                    case "text":

                            newcell.childNodes[0].value = "";
                            break;
                    case "checkbox":
                            newcell.childNodes[0].checked =
false;
                            break;
                    case "select-one":
                            newcell.childNodes[0].selectedIndex =
0;
                            break;
```

```
                }
            }
        }

        function deleteRow(tableID) {
            try {
            var table = document.getElementById(tableID);
            var rowCount = table.rows.length;
            alert("js called "+rowCount);
            for(var i=0; i<rowCount; i++) {
                var row = table.rows[i];
                var chkbox = row.cells[0].childNodes[0];
                if(null != chkbox && true == chkbox.checked) {
                    if(rowCount <= 1) {
                        alert("Cannot delete all the rows.");
                        break;
                    }
                    table.deleteRow(i);
                    rowCount--;
                    i--;
                }


            }
            }catch(e) {
                alert(e);
            }
        }

    </SCRIPT>
    <script type="text/javascript">
      function altRows(id) {
            if (document.getElementsByTagName) {

                  var table = document.getElementById(id);
                  var rows = table.getElementsByTagName("tr");
                  for (var i = 0; i < rows.length; i++) {
                        if (i % 2 == 0) {
                              rows[i].className = "evenrowcolor";
                        } else {
                              rows[i].className = "oddrowcolor";
                        }
                  }
            }
      }
      window.onload = function() {
            altRows('alternatecolor');
      }
</script>
            <title>
                  Register Item Purchased
            </title>
```

```
      </head>
      <% if (request.getSession().getAttribute("loginName") ==
null) {

      request.getRequestDispatcher("sessionExpaire.jsp")
                  .forward(request, response);

} else {
      String message="";
      if (request.getAttribute("message")==null){
               message= "";
      }else{
             message= (String) request.getAttribute("message");
      }
      if (message.compareToIgnoreCase("Operation is
successful")==0){
            errorColor="Blue";
      }else{
            errorColor="Red";
      }%>
      <body bgcolor="#F8FAFF">
            <!-- <div id="container"> -->
            <div id="container"style="width:800px">
            <div style="width:800px; background-color: #66A666;
color: white" align="center">
                  <h4>Item Purchased</h4>
            </div>
            <form method="post" action="<%=path +
"displaypostobligation"%>">
                  <table width="800px" border="0" align="center"
class="customers"  bgcolor= #F0FFFF  id="alternatecolor"
valign="top">
                        <tr><th>GRN :</th><td><input type="number"
name="grn" id="grn"maxlength="6" required /></td></tr>
                        <tr><th>Supplier Name: </th><td><input
type="text" name="grn" id="grn"maxlength="6" required
/></td></tr>
</TD>
</tr>
<tr><th>Purchased Date: </th><td><input type="date"
name="purchase_date" required
placeholder="dd/mm/yyyy"/></td></tr>
<tr><td><INPUT type="button" value="Add Row"
onclick="addRow('dataTable')" /></td>
 <td><INPUT type="button" value="Delete Row"
onclick="deleteRow('dataTable')" /></td></tr>
</table>
 <table align="center"  width="800px" border="0" bgcolor= #AEDCF2
class="customers">
  <tr>
   <th align="center">No</th>
```

```
   <th align="center">Item Name</th>
   <th align="center">Item Description</th>
   <th align="center">Unit Price</th>
   <th align="center">Quantity</th>
   <th align="center">Warranty Period</th>
   </tr>
      </table>
       <table align="center" id="dataTable" width="800px"
border="0"  bgcolor=#E0F5FF   class="customers">
       <tr> <TD align="center"><INPUT type="checkbox" name="chk"
id="chk" /></TD>
            <td ><input type="text" name="grn"
id="grn"maxlength="6" required />
        </td>
        <td align="center"><input type="text"
name="item_description" id="item_description" required /></td>
                     <td align="center"><div style="margin-
right: 3px;"><div style="padding-right: 3px;"><input
type="number" name="unit_price" id="unit_price"step="any"
style="width:50%;"required/></div></div></td>
                     <td align="center"><div style="margin-
right: 3px;"><div style="padding-right: 3px;"><input
type="number" name="quantity" id="quantity"
style="width:50%;align:center;"required/></div></div></td>
                     <td align="center"><div style="margin-
right: 3px;"><div style="padding-right: 3px;"><input
type="number" name="warranty_period" id="warranty_period"
style="width:50%;"value="0"/></div></div></td></tr>
      </table>
      <table align="center" width="800px" border="0"
bgcolor=#E0F5FF   class="customers">
      <tr>
      <td align="center"><input type="submit" value="Authorize
item details"></td>
      <td align="center"><input type="reset" value="Cancel"></td>
      </tr>

      <% if(message!=""){%>
                     <tr><td colspan="2"><font face="verdana"
color="<%=errorColor%>"><%=message%></font></td></tr>

                     <%} %>
      </table>
       </form>
      </div>
      </body>
      <%message="";} %>
</html>
```

```
package com.dbe.fam.control;

import java.io.IOException;
import javax.servlet.ServletException;
import javax.servlet.annotation.WebServlet;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

/**
 * Servlet implementation class displayauthorizeitemsole
 */
@WebServlet("/displayauthorizeitemsoleserv")
public class displayauthorizeitemsole extends HttpServlet {
	private static final long serialVersionUID = 1L;

    /**
     * @see HttpServlet#HttpServlet()
     */
    public displayauthorizeitemsole() {
        super();
        // TODO Auto-generated constructor stub
    }

	/**
	 * @see HttpServlet#doGet(HttpServletRequest request, HttpServletResponse
response)
	 */
	protected void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {
		// TODO Auto-generated method stub
	}

	/**
	 * @see HttpServlet#doPost(HttpServletRequest request, HttpServletResponse
response)
	 */
	protected void doPost(HttpServletRequest request, HttpServletResponse
response) throws ServletException, IOException {
		// TODO Auto-generated method stub
		response.sendRedirect("jsp/soleauthorize.jsp");
	}

}
package com.dbe.fam.control;
```

```
import java.io.IOException;
import javax.servlet.ServletException;
import javax.servlet.annotation.WebServlet;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

/**
 * Servlet implementation class displayinfoplicytraining
 */
@WebServlet("/displayinfoplicytrainingserv")
public class displayinfoplicytraining extends HttpServlet {
	private static final long serialVersionUID = 1L;

    /**
     * @see HttpServlet#HttpServlet()
     */
    public displayinfoplicytraining() {
        super();
        // TODO Auto-generated constructor stub
    }

	/**
	 * @see HttpServlet#doGet(HttpServletRequest request, HttpServletResponse
response)
	 */
	protected void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {
		// TODO Auto-generated method stub
	}

	/**
	 * @see HttpServlet#doPost(HttpServletRequest request, HttpServletResponse
response)
	 */
	protected void doPost(HttpServletRequest request, HttpServletResponse
response) throws ServletException, IOException {
		// TODO Auto-generated method stub
		//request.setAttribute("message", errorMessage);

		//request.setAttribute("checkPath", checkPath);
		String[] reason=request.getParameterValues("reason");
		request.setAttribute("reason", reason);
```

```
		request.getRequestDispatcher("jsp/listselectedreason.jsp").forward(request,respon
se);

		}

}

package com.dbe.fam.control;

import java.io.IOException;
import javax.servlet.ServletException;
import javax.servlet.annotation.WebServlet;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

/**
 * Servlet implementation class displayinfoplicytrainingfull
 */
@WebServlet("/displayinfoplicytrainingfullserv")
public class displayinfoplicytrainingfull extends HttpServlet {
		private static final long serialVersionUID = 1L;

    /**
     * @see HttpServlet#HttpServlet()
     */
    public displayinfoplicytrainingfull() {
        super();
        // TODO Auto-generated constructor stub
    }

		/**
		 * @see HttpServlet#doGet(HttpServletRequest request, HttpServletResponse
response)
		 */
		protected void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {
			// TODO Auto-generated method stub
		}

		/**
		 * @see HttpServlet#doPost(HttpServletRequest request, HttpServletResponse
response)
		 */
```

```
	protected void doPost(HttpServletRequest request, HttpServletResponse
response) throws ServletException, IOException {
		// TODO Auto-generated method stub
		response.sendRedirect("jsp/listallreason.jsp");
	}

}

package com.dbe.fam.control;

import java.io.IOException;
import javax.servlet.ServletException;
import javax.servlet.annotation.WebServlet;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

/**
 * Servlet implementation class displaypostobligation
 */
@WebServlet("/displaypostobligationserv")
public class displaypostobligation extends HttpServlet {
	private static final long serialVersionUID = 1L;

    /**
     * @see HttpServlet#HttpServlet()
     */
    public displaypostobligation() {
        super();
        // TODO Auto-generated constructor stub
    }

	/**
	 * @see HttpServlet#doGet(HttpServletRequest request, HttpServletResponse
response)
	 */
	protected void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {
		// TODO Auto-generated method stub
	}

	/**
	 * @see HttpServlet#doPost(HttpServletRequest request, HttpServletResponse
response)
	 */
```

```
	protected void doPost(HttpServletRequest request, HttpServletResponse
response) throws ServletException, IOException {
		// TODO Auto-generated method stub
		response.sendRedirect("jsp/postobligation.jsp");
	}

}
```

APPENDIX D: Code for prototype version II

The codes below are the changes made in the first version of the prototype

```
<%@ page language="java" contentType="text/html; charset=ISO-
8859-1"
     pageEncoding="ISO-8859-1"%>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>CheckerMenu</title>
<script type="text/javascript"
src="../javascripts/jquery.min.js"></script>
<script type="text/javascript"
src="../javascripts/animatedcollapse.js"></script>
<script type="text/javascript" language="javascript"
     src="../javascripts/jquery.js"></script>
<link type="text/css" rel="stylesheet" href="../css/styles.css"
/>
<script type="text/javascript">
     $(document).ready(
                function() {
                     //slides the element with class "menu_body"
when paragraph with class "menu_head" is clicked
                     $("#secondary p.menu_head").click(
                               function() {
                                    $(this).css({
                                         backgroundImage :
"url(image/down.png)"

     }).next("div.menu_body").slideToggle(300).siblings(

     "div.menu_body").slideUp("slow");
                                    $(this).siblings().css({
                                         backgroundImage :
"url(image/left.png)"
                                    });
                               });
                });
</script>
</head>
<%
     if (request.getSession().getAttribute("loginName") == null)
{


     request.getRequestDispatcher("sessionExpaire.jsp").forward(
                     request, response);
```

```
      } else {
%>

<body bgcolor="#F8FAFF">

      <div id="bd">
            <div id="secondary" class="menu_list">
                  <p class="menu_head">Authorizer</p>
                  <div class="menu_body">
                        <a href="authorizevehiclerecords.jsp"
target="content" target="content">authorize vehicle</a>
                        <a href="authorizeitempurchasedrecords.jsp"
target="content" target="content">authorize item purchased</a>
                        <a href="authorizeitemrequestedrecords.jsp"
target="content" target="content">authorize item requested</a>
                        <a
href="authorizeitemdistributedrecords.jsp" target="content"
target="content">authorize item distributed</a>
                        <a href="listofatriskinsiders.jsp"
target="content" target="content">Anonymized list of suspected
insiders</a>
                        <a href="behaviourofinsiders.jsp"
target="content" target="content">Anonymized report on Behaviour
insiders</a>
                        <a href="newbehaviours.jsp"
target="content" target="content">New Behaviours learned</a>
                  </div>
            </div>
      </div>
</body>
<%
      }
%>
</html>

<%@ page language="java" contentType="text/html; charset=ISO-
8859-1" %>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>New Behaviours learned</title>
<link rel="stylesheet" href="../css/structure.css"
type="text/css" />
<link rel="stylesheet" href="../css/form.css" type="text/css" />
<link rel="stylesheet" href="../css/theme.css" type="text/css" />
<link rel="stylesheet" href="../css/viewTable.css"
type="text/css"></link>

<script type="text/javascript">
      function altRows(id) {
```

```
            if (document.getElementsByTagName) {

                  var table = document.getElementById(id);
                  var rows = table.getElementsByTagName("tr");

                  for (i = 0; i < rows.length; i++) {
                        if (i % 2 == 0) {
                              rows[i].className = "evenrowcolor";
                        } else {
                              rows[i].className = "oddrowcolor";
                        }
                  }
            }
      }
      window.onload = function() {
            altRows('alternatecolor');
      }
</script>
</head>
<body>
<form name=myform>
<table class="report" id="alternatecolor" align="center">
    <tr>
        <td colspan="6" align="center" style="background-
color:#76AC78;color:#0000FF;"><b>New Behaviours learned</b></td>
    </tr>
    <tr style="background-color: #efefef;">
        <th><b>New Behaviour</b></th>
        <th><b>Component</b></th>
    </tr>
 <tr><td>Mouse press changes with stress</td><td>Motive</td></tr>
 <tr><td>The number of application opened at a time changes with
insiders</td><td>Motive</td></tr>
 </table>
</form>
</body></html>
```

APPENDIX E: Website for prototype and research data

Both versions of the prototype and the research data for two iterations is available on website, https://sites.google.com/site/ppcaitppdata/.

APPENDIX F: Ethical Clearance

UNISA | college of science, engineering and technology

Dear Mr. Solomon Mekonnen Tekle (49026526)

Date: 2016-02-08

Application number:
001/SMT/2016/CSET_SOC

REQUEST FOR ETHICAL CLEARANCE: (A Privacy-Preserving Context-Aware Insider Threat Prevention and Prediction model)

Please note that you cannot use this certificate to collect data from Unisa but you will need further clearance from SRIHDC.

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your research study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CRIC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

Please note that the ethical clearance is granted for the duration of this project and if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

RECEIVED
2016 -02- 0 8
OFFICE OF THE EXECUTIVE DEAN
College of Science, Engineering and Technology

Prof Ernest Mnkandla
Chair: College of Science, Engineering and Technology Ethics Sub-Committee

Prof IOG Mocke
Executive Dean: College of Science, Engineering and Technology

APPENDIX G: Certificate of editing

TO WHOM IT MAY CONCERN

I, Yvonne Smuts, hereby declare that I have edited the thesis, with the exception of the appendices, of Solomon Mekonnen Tekle to be submitted in accordance with the requirements for the degree of Doctor of Philosophy in the subject of Information Systems at the University of South Africa, and that it adheres to the standard and level of quality set for such a text.

Yours faithfully

(Ms) Y Smuts Date: 21 September 2017

BA (Languages) HED (cum laude) (UP)
Language editor/translator

APPENDIX H: Publications from this research

Mekonnen, S., Padayachee, K., & Meshesha, M. (2015, November). A Privacy-Preserving, Context-Aware, Insider Threat Prediction and Prevention Model Predicated on the Components of the Fraud Diamond. In *Information and Computer Technology (GOCICT), 2015 Annual Global Online Conference on* (pp. 60-65). IEEE.